

Installationshandbuch

Revision B

McAfee® Email Gateway 7.x – Virtual Appliances

Inhaltsverzeichnis

Einleitung

Dieses Handbuch enthält die Informationen, die Sie zum Installieren Ihres McAfee-Produkts benötigen.

Inhalt

Informationen zu diesem Handbuch

In diesem Abschnitt werden die Zielgruppe des Handbuchs, die verwendeten typografischen Konventionen und Symbole sowie die Gliederung des Handbuchs beschrieben.

Zielgruppe

Die Dokumentation von McAfee wird inhaltlich sorgfältig auf die Zielgruppe abgestimmt.

Die Informationen in diesem Handbuch richten sich in erster Linie an:

- **Administratoren** – Personen, die das Sicherheitsprogramm eines Unternehmens implementieren und umsetzen.

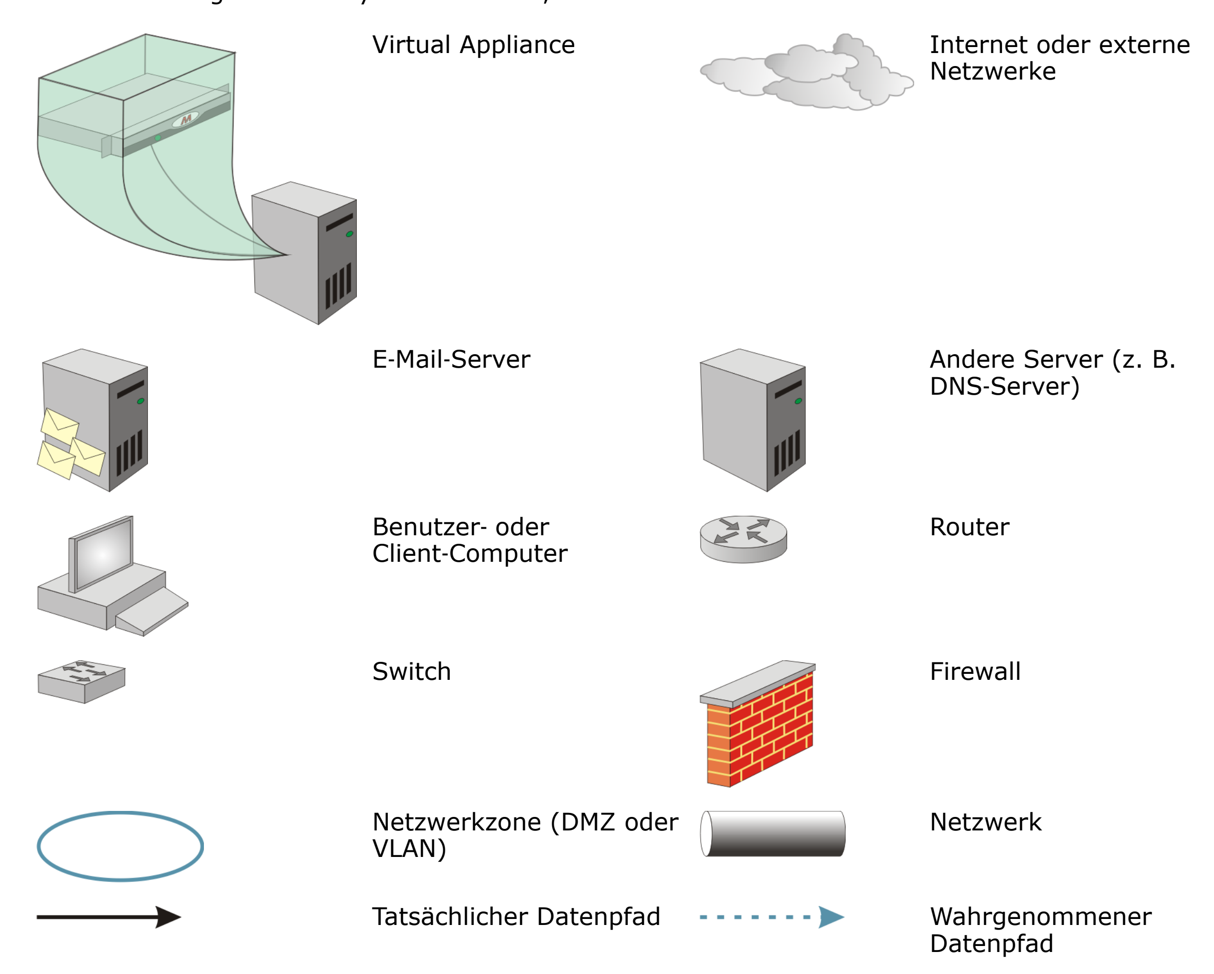
Konventionen

In diesem Handbuch werden folgende typografische Konventionen und Symbole verwendet.

Buchtitel, *Begriff*, *Hervorhebung*	Titel eines Buchs, Kapitels oder Themas; ein neuer Begriff; eine Hervorhebung.
Fett	Text, der stark hervorgehoben wird.
`Benutzereingabe, Code, Meldung`	Befehle oder andere Texte, die vom Benutzer eingegeben werden; ein Code-Beispiel; eine angezeigte Meldung.
Benutzeroberflächentext	Wörter aus der Benutzeroberfläche des Produkts, z. B. Optionen, Menüs, Schaltflächen und Dialogfelder.
Hypertext-Blau	Ein Link auf ein Thema oder eine externe Website.
	Hinweis: Zusätzliche Informationen, beispielsweise eine alternative Methode für den Zugriff auf eine Option.
	Tipp: Vorschläge und Empfehlungen.
	Wichtig/Vorsicht: Wichtige Ratschläge zum Schutz Ihres Computersystems, der Software-Installation, des Netzwerks, Ihres Unternehmens oder Ihrer Daten.
	Warnung: Wichtige Ratschläge, um körperliche Verletzungen bei der Nutzung eines Hardware-Produkts zu vermeiden.

Graphische Konventionen

Lernen Sie die grafischen Symbole kennen, die in diesem Dokument verwendet werden.



Definition der Begriffe in diesem Handbuch

Lernen Sie einige der Schlüsselbegriffe kennen, die in diesem Dokument verwendet werden.

Begriff	Beschreibung
Demilitarisierte Zone (DMZ)	Ein Computer-Host oder kleineres Netzwerk, das als Puffer zwischen ein privates Netzwerk und das äußere öffentliche Netzwerk eingefügt wurde, um den direkten Zugriff durch außenstehende Benutzer auf Ressourcen im privaten Netzwerk zu verhindern.
DAT-Dateien	Erkennungsdefinitionsdateien (DAT), auch als Signaturdateien bezeichnet, enthalten die Definitionen, die Viren, Trojaner, Spyware, Adware und andere potenziell unerwünschte Programme (PUPe) identifizieren, erkennen und entfernen.
Betriebsmodus	Es gibt drei Betriebsmodi für das Produkt: "Expliziter Proxy", "Transparente Bridge" und "Transparenter Router".

Begriff	Beschreibung
Richtlinie	Eine Sammlung der Sicherheitskriterien (z. B. Konfigurationseinstellungen, Benchmarks und Spezifikationen für den Netzwerkzugriff), die die erforderliche Compliance-Stufe für Benutzer, Geräte und Systeme definieren, die von einer McAfee-Sicherheitsanwendung bewertet oder erzwungen werden kann.
Reputationsdienst-Prüfung	Teil der Absenderauthentifizierung. Wenn ein Absender die Reputationsdienst-Prüfung nicht besteht, ist die Appliance so eingestellt, dass die Verbindung beendet und die Nachricht nicht zugelassen wird. Die IP-Adresse des Absenders wird zu einer Liste blockierter Verbindungen hinzugefügt und in Zukunft automatisch auf Kernel-Ebene blockiert.

Verwendung dieses Handbuchs

Dieser Abschnitt enthält eine kurze Zusammenfassung der in diesem Dokument enthaltenen Informationen.

In diesem Handbuch wird Folgendes behandelt:

- Planung und Ausführung Ihrer Installation.
- Umgang mit der Benutzeroberfläche.
- Testen der ordnungsgemäßen Funktion des Produkts.
- Anwendung der aktuellsten Erkennungsdefinitionsdateien.
- Vertrautmachen mit einigen Scan-Richtlinien, Erstellen von Berichten und Abrufen der Statusinformationen.
- Beheben einiger grundlegender Probleme.

Weitere Informationen über die Scan-Funktionen des Produkts finden Sie in der Online-Hilfe des Produkts und in der aktuellen Version des *McAfee Email Gateway-Administratorhandbuches*.

Quellen für Produktinformationen

McAfee stellt Ihnen die Informationen zur Verfügung, die Sie in den einzelnen Phasen der Produktimplementierung benötigen – von der Installation bis hin zur täglichen Nutzung und Fehlerbehebung. Nach der Produktveröffentlichung erhalten Sie Informationen zu diesem Produkt online in der KnowledgeBase von McAfee.

Vorgehensweise

1. Wechseln Sie zum McAfee Technical Support ServicePortal unter http://mysupport.mcafee.com.
2. Greifen Sie unter **Self Service** (Online-Support) auf die erforderlichen Informationen zu:

Zugriff auf	Vorgehensweise
Benutzerdokumentation	1 Klicken Sie auf **Product Documentation** (Produktdokumentation). 2 Wählen Sie ein Produkt und dann eine Version aus. 3 Wählen Sie ein Produktdokument aus.
KnowledgeBase	• Klicken Sie auf **Search the KnowledgeBase** (KnowledgeBase durchsuchen), um Antworten auf Ihre produktbezogenen Fragen zu erhalten. • Klicken Sie auf **Browse the KnowledgeBase** (KnowledgeBase durchblättern), um Artikel nach Produkt und Version aufzulisten.

1 Einführung in McAfee Email Gateway Virtual Appliance

Die McAfee Email Gateway Virtual Appliance bietet Unternehmen umfassenden Schutz gegen E-Mail-Bedrohungen.

McAfee Email Gateway Virtual Appliance funktioniert in folgenden virtuellen Umgebungen:

- VMware vSphere 4.x oder höher
- VMware vSphere Hypervisor (ESXi) 4.x oder höher

Umfang des Download-Pakets

Die McAfee Email Gateway Virtual Appliance wird in einer ZIP-Datei zur Verfügung gestellt, die die Software-Installationsdateien und Installationsdokumente zur Installation der virtuellen Appliance auf VMware vSphere 4.x enthält.



Das Download-Paket enthält keine Installationsdateien für das VMware-Produkt. Wenn Sie Ihre virtuelle Software noch nicht eingerichtet haben, gehen Sie zur VMware-Website (http://www.vmware.com), um VMware vSphere oder VMware vSphere Hypervisor (ESXi) zu erwerben.

2 Vorbereitung der Installation

Um den sicheren Betrieb Ihres McAfee Email Gateway Virtual Appliance zu gewährleisten, sollten Sie folgende Punkte vor Beginn der Installation bedenken.

- Machen Sie sich mit den Betriebsmodi und den Funktionen vertraut. Es ist wichtig, dass Sie eine gültige Konfiguration auswählen.
- Entscheiden Sie, wie Sie die Appliance in Ihr Netzwerk integrieren möchten, und stellen Sie fest, welche Informationen Sie benötigen, bevor Sie beginnen. Sie benötigen beispielsweise den Namen und die IP-Adresse des Geräts.

Inhalt

Nicht bestimmungsgemäße Nutzung

Erfahren Sie, wie Sie vermeiden, das Produkt nicht bestimmungsgemäß zu nutzen.

McAfee Email Gateway Virtual Appliance ist:

- **Keine Firewall** – Es muss in Ihrer Organisation hinter einer ordnungsgemäß konfigurierten Firewall verwendet werden.
- **Kein Server zum Speichern zusätzlicher Software und Dateien** – Installieren Sie keine Software auf dem Gerät, und fügen Sie keine zusätzlichen Dateien hinzu, es sei denn, Sie werden in der Produktdokumentation oder von Ihrem Support-Mitarbeiter dazu aufgefordert.



Das Gerät kann nicht alle Arten von Datenverkehr verarbeiten. Wenn Sie den Modus „Expliziter Proxy" verwenden, sollten nur Protokolle an das Gerät gesendet werden, die gescannt werden müssen.

Überlegungen zu Netzwerkmodi

In diesem Abschnitt lernen Sie die Betriebsmodi (Netzwerkmodi) kennen, in denen das Gerät betrieben werden kann.

Bevor Sie das McAfee Email Gateway konfigurieren, müssen Sie sich überlegen, welchen Netzwerkmodus Sie verwenden möchten. Vom ausgewählten Modus hängt es ab, wie Sie Ihren **VMware ESX**-Host physisch an Ihr Netzwerk anschließen. Verschiedene Modi wirken sich auch auf die Konfiguration Ihres vSwitch aus, an den Ihre virtuelle Appliance angeschlossen wird. Die Ausführung der virtuellen Appliance im Modus "Expliziter Proxy" erfordert den geringsten Konfigurationsaufwand

auf dem VMware ESX-Host und ist leichter einzurichten. Für die Installation der virtuellen Appliance in einem der transparenten Modi müssen andere Überlegungen getroffen werden. Im Folgenden werden alle erforderlichen Schritte für die ESX-Konfiguration in einem der beiden Modi beschrieben.

Sie können einen der folgenden Netzwerkmodi auswählen:

- **Modus "Expliziter Proxy"** – Die virtuelle Appliance fungiert als Proxyserver und Mail-Relay.
- **Modus "Transparenter Router"** – Die virtuelle Appliance fungiert als Router.
- **Modus "Transparente Bridge"** – Die virtuelle Appliance fungiert als Ethernet-Bridge.

Wenn Sie nach der Lektüre dieses und der folgenden Abschnitte weiterhin unsicher sind, welchen Modus Sie verwenden sollen, sprechen Sie mit einem Netzwerkexperten.

Modus "Expliziter Proxy"

In diesem Abschnitt lernen Sie den Modus "Expliziter Proxy" des McAfee Email Gateways besser kennen.

Im Modus "Expliziter Proxy" müssen einige Netzwerkgeräte so eingerichtet werden, dass sie Datenverkehr explizit an das Gerät senden. Das Gerät fungiert dann als Proxy oder Relay und verarbeitet den Datenverkehr für die Geräte.

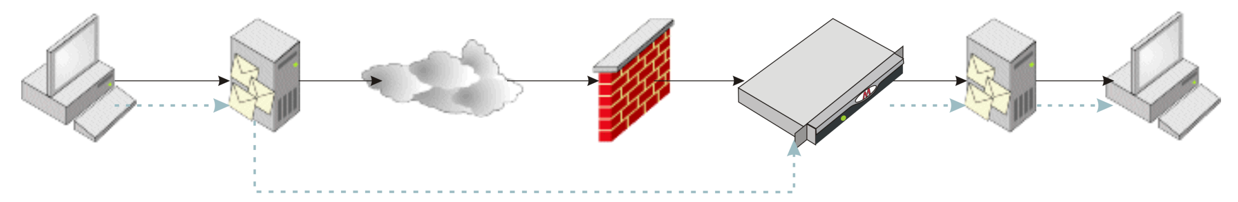


Abbildung 2-1 Modus "Expliziter Proxy" – sichtbarer Datenpfad

Der Modus "Expliziter Proxy" ist am besten für Netzwerke geeignet, in denen Client-Geräte über ein einzelnes Upstream- und Downstream-Gerät eine Verbindung zum Gerät herstellen.



Dies ist möglicherweise nicht die beste Option, wenn verschiedene Netzwerkgeräte erneut konfiguriert werden müssen, damit sie den Datenverkehr an das Gerät senden.

Netzwerk- und Gerätekonfiguration

Wenn sich das Gerät im Modus "Expliziter Proxy" befindet, müssen Sie den internen Mail-Server explizit so konfigurieren, dass er E-Mail-Verkehr an das Gerät sendet. Das Gerät prüft den E-Mail-Verkehr, bevor es ihn im Namen des Absenders an den externen Mail-Server weiterleitet. Der externe E-Mail-Server leitet die E-Mail dann an den Empfänger weiter.

Entsprechend muss das Netzwerk so konfiguriert werden, dass eingehende E-Mail-Nachrichten aus dem Internet nicht dem internen Mail-Server, sondern dem Gerät zugestellt werden.

Das Gerät kann den E-Mail-Verkehr dann prüfen, bevor es ihn im Namen des Absenders an den internen E-Mail-Server zur Zustellung weiterleitet, wie in der Abbildung dargestellt.

Beispielsweise kann ein externer Mail-Server direkt mit dem Gerät kommunizieren, auch wenn der Datenverkehr möglicherweise mehrere Netzwerkserver passiert, bevor er das Gerät erreicht. Der wahrgenommene Pfad verläuft vom externen Mail-Server zum Gerät.

Protokolle

Um ein unterstütztes Protokoll zu scannen, müssen Sie Ihre anderen Netzwerkserver oder Client-Computer so konfigurieren, dass das Protokoll durch das Gerät geleitet wird, sodass kein Datenverkehr das Gerät umgehen kann.

Firewall-Regeln

Im Modus "Expliziter Proxy" werden alle Firewall-Regeln, die für den Client-Zugriff auf das Internet eingerichtet wurden, außer Kraft gesetzt. Für die Firewall sind nur die physischen IP-Adressinformationen für das Gerät sichtbar, nicht jedoch die IP-Adressen der Clients. Die Firewall kann daher ihre Internetzugriffsregeln nicht auf die Clients anwenden.

Stellen Sie sicher, dass die Firewall-Regeln aktualisiert werden. Die Firewall muss den Datenverkehr vom McAfee® Email Gateway akzeptieren, darf aber keinen Datenverkehr verarbeiten, der direkt von den Client-Geräten kommt.

Richten Sie Firewall-Regeln ein, die verhindern, dass unerwünschter Datenverkehr in Ihr Unternehmen gelangt.

Platzieren des Geräts

Konfigurieren Sie die Netzwerkgeräte so, dass der zu scannende Datenverkehr an das McAfee® Email Gateway gesendet wird. Das ist wichtiger als der Standort des McAfee® Email Gateway.

Der Router muss allen Benutzern erlauben, eine Verbindung zum McAfee® Email Gateway herzustellen.

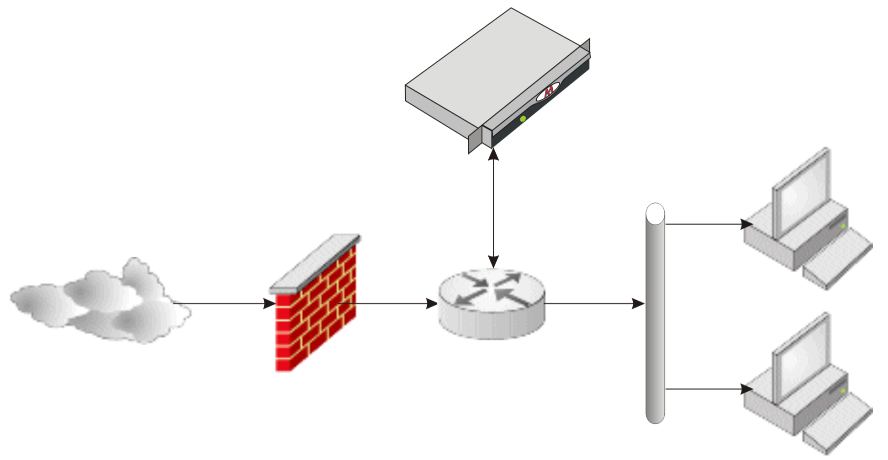


Abbildung 2-2 Platzierung im Modus "Expliziter Proxy"

Das McAfee® Email Gateway muss innerhalb Ihres Unternehmens hinter einer Firewall platziert werden, wie in Abbildung 6 dargestellt: Konfiguration als expliziter Proxy.

Normalerweise ist die Firewall so konfiguriert, dass der Datenverkehr, der nicht direkt von dem Gerät stammt, gesperrt wird. Wenn Sie in Bezug auf die Topologie Ihres Netzwerks unsicher sind und nicht wissen, wie Sie das Gerät integrieren sollen, wenden Sie sich an Ihren Netzwerkspezialisten.

Verwenden Sie diese Konfiguration in folgenden Fällen:

- Das Gerät wird im Modus "Expliziter Proxy" betrieben.
- Sie verwenden E-Mail (SMTP).

Für diese Konfiguration gilt:

- Konfigurieren Sie die externen DNS-Server (Domain Name System) oder NAT (Network Address Translation) auf der Firewall so, dass der externe Mail-Server E-Mails an das Gerät zustellt, nicht an den internen Mail-Server.
- Konfigurieren Sie die internen Mail-Server so, dass E-Mail-Verkehr an das Gerät gesendet wird. Das heißt, die internen Mail-Server müssen das Gerät als Smart-Host verwenden. Vergewissern Sie sich, dass die Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.
- Stellen Sie sicher, dass die Firewall-Regeln aktualisiert werden. Die Firewall muss den Datenverkehr von dem Gerät akzeptieren, darf aber keinen Datenverkehr verarbeiten, der direkt von den Client-Geräten kommt. Richten Sie Regeln ein, die verhindern, dass unerwünschter Datenverkehr in Ihr Unternehmen gelangt.

Modus "Transparente Bridge"

In diesem Abschnitt lernen Sie den Modus "Transparente Bridge" des McAfee Email Gateways besser kennen.

Im Modus "Transparente Bridge" bemerken die kommunizierenden Server das Gerät nicht. Der Betrieb des Geräts ist für die Server transparent.

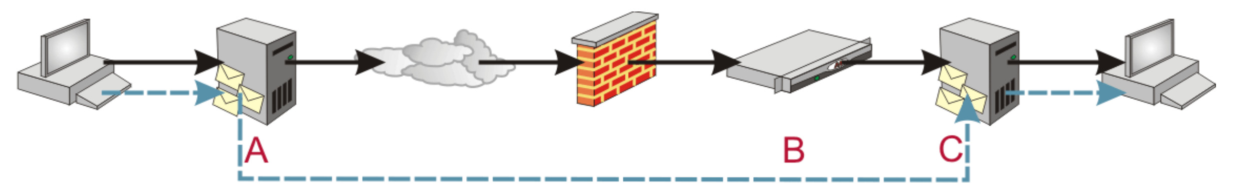


Abbildung 2-3 Modus "Transparente Bridge" – sichtbarer Datenpfad

In der Abbildung sendet der externe E-Mail-Server (**A**) E-Mail-Nachrichten an den internen E-Mail-Server (**C**). Der externe Mail-Server kann nicht erkennen, dass die von ihm gesendete E-Mail-Nachricht vom Gerät abgefangen und gescannt wird (**B**).

Der externe E-Mail-Server scheint direkt mit dem internen E-Mail-Server zu kommunizieren (der Pfad wird als gestrichelte Linie dargestellt). Tatsächlich wird der Datenverkehr möglicherweise durch mehrere Netzwerkgeräte geleitet und vom Gerät abgefangen und gescannt, bevor er den internen Mail-Server erreicht.

Arbeitsweise des Geräts im Modus "Transparente Bridge"

Im Modus "Transparente Bridge" wird das Gerät über den LAN1- und den LAN2-Anschluss mit dem Netzwerk verbunden. Das Gerät scannt den empfangenen Datenverkehr und fungiert als Bridge, die zwei Netzwerksegmente verbindet, behandelt diese aber wie ein einziges logisches Netzwerk.

Konfiguration im Modus "Transparente Bridge"

Der Modus "Transparente Bridge" erfordert weniger Konfigurationsaufwand als die Modi "Transparenter Router" oder "Expliziter Proxy". Sie müssen nicht alle Clients, das Standard-Gateway, MX-Einträge, Firewall-NAT und E-Mail-Server neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Da das Gerät in diesem Modus nicht als Router fungiert, ist es auch nicht erforderlich, eine Routing-Tabelle zu aktualisieren.

Platzieren des Geräts bei Betrieb im Modus "Transparente Bridge"

Aus Sicherheitsgründen sollten Sie das Gerät innerhalb Ihres Unternehmens und hinter einer Firewall betreiben.

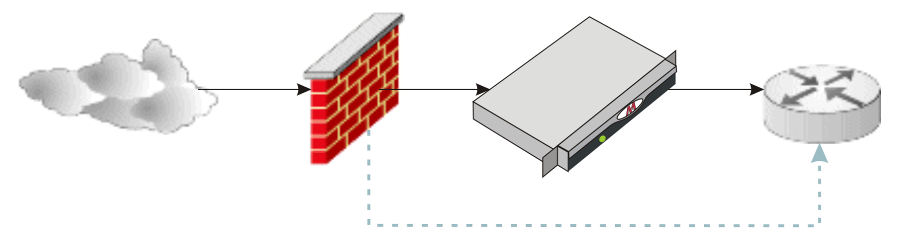


Abbildung 2-4 Platzierung im Modus "Transparente Bridge"



Platzieren Sie das Gerät im Modus "Transparente Bridge" zwischen der Firewall und Ihrem Router, wie in der Abbildung dargestellt.

In diesem Modus verbinden Sie zwei Netzwerksegmente physisch mit dem Gerät. Das Gerät behandelt diese als eine einzige logische Einheit. Da sich die Geräte – Firewall, Gerät und Router – im selben logischen Netzwerk befinden, müssen sie kompatible IP-Adressen im selben Subnetz haben.

Geräte auf der einen Seite der Bridge (z. B. ein Router), die mit den Geräten auf der anderen Seite der Bridge (z. B. einer Firewall) kommunizieren, bemerken die Bridge nicht. Sie erkennen nicht, dass der Datenverkehr abgefangen und gescannt wird. Deshalb wird dieser Betriebsmodus des Geräts als "Transparente Bridge" bezeichnet.

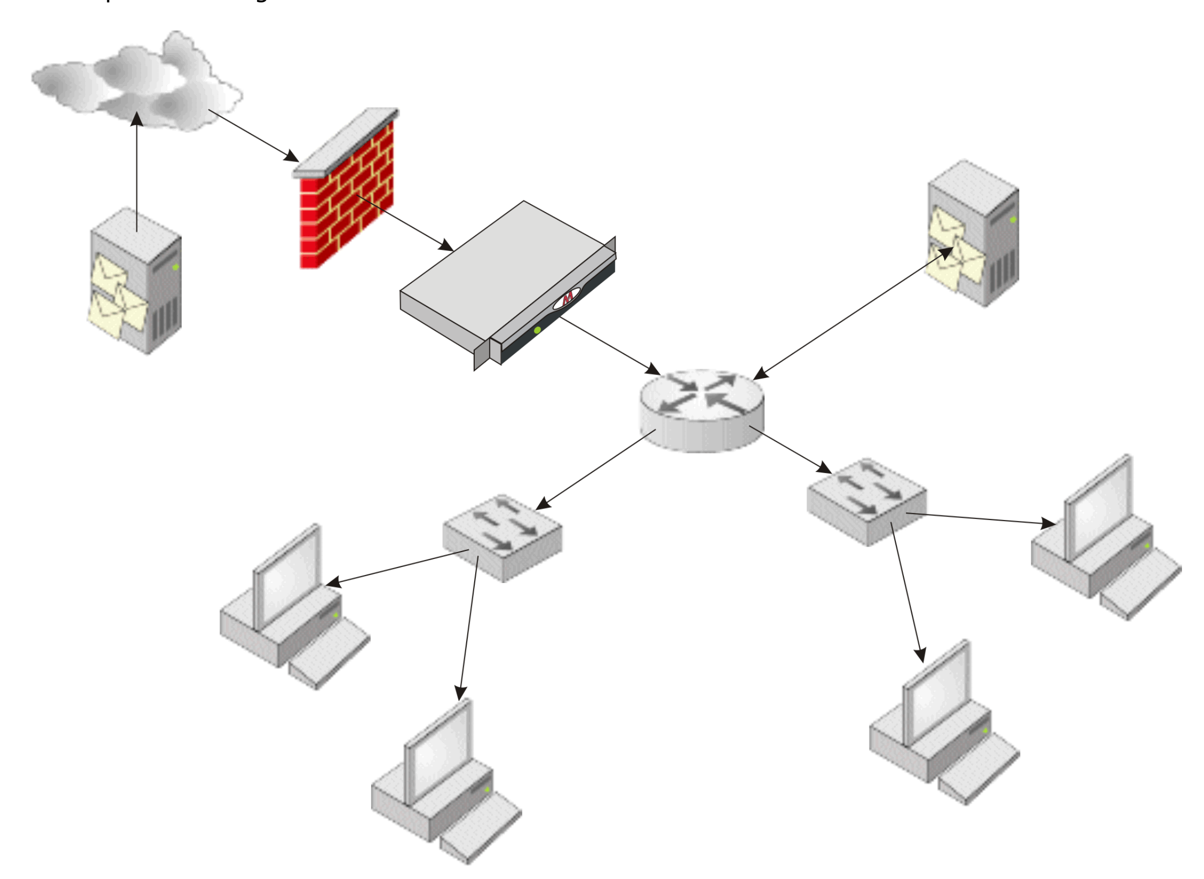


Abbildung 2-5 Netzwerkstruktur – Modus "Transparente Bridge"

Modus "Transparenter Router"

In diesem Abschnitt lernen Sie den Modus "Transparenter Router" des McAfee Email Gateways besser kennen.

Im Modus "Transparenter Router" scannt das Gerät den E-Mail-Verkehr zwischen zwei Netzwerken. Das Gerät hat eine IP-Adresse für ausgehenden gescannten Verkehr und muss eine IP-Adresse für eingehenden Verkehr haben.

Die kommunizierenden Netzwerkserver erkennen nicht, dass das Gerät zwischengeschaltet ist. Der Betrieb des Geräts ist für die Geräte transparent.

Arbeitsweise des Geräts im Modus "Transparente Router"

Im Modus "Transparenter Router" wird das Gerät mit den Netzwerken über den LAN1- und den LAN2-Anschluss verbunden. Das Gerät scannt den Datenverkehr, der über ein Netzwerk eingeht, und leitet ihn an das nächste Netzwerkgerät in einem anderen Netzwerk weiter. Das Gerät fungiert als Router (wobei es Datenverkehr zwischen den verschiedenen Netzwerken auf der Basis der Informationen in den Routing-Tabellen weiterleitet).

Konfiguration im Modus "Transparenter Router"

Im Modus "Transparenter Router" müssen Sie Ihre Netzwerkgeräte nicht explizit neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Sie müssen lediglich die Routing-Tabelle für das Gerät konfigurieren und einige der Routing-Informationen für die Netzwerkgeräte auf einer Seite des Geräts ändern (der Geräte also, die an die LAN1- und LAN2-Anschlüsse des Geräts angeschlossen sind). Es könnte zum Beispiel erforderlich sein, das Gerät als Standard-Gateway zu konfigurieren.

Im Modus "Transparenter Router" muss das Gerät zwei Netzwerke miteinander verbinden. Das Gerät muss innerhalb Ihres Unternehmens hinter einer Firewall platziert werden.



Im Modus "Transparenter Router" werden weder Multicast-IP-Datenverkehr noch andere Protokolle wie NETBEUI und IPX (Nicht-IP-Protokolle) unterstützt.

Firewall-Regeln

Im Modus "Transparenter Router" wird die Firewall mit der physischen IP-Adresse für die LAN1/LAN2-Verbindung mit dem Management-Blade-Server verbunden.

Platzieren des Geräts

Verwenden Sie das Gerät im Modus "Transparenter Router", um einen im Netzwerk vorhandenen Router zu ersetzen.



Wenn Sie den Modus "Transparenter Router" verwenden und keinen vorhandenen Router ersetzen, müssen Sie einen Teil Ihres Netzwerks neu konfigurieren, damit der Datenverkehr korrekt durch das Gerät fließt.

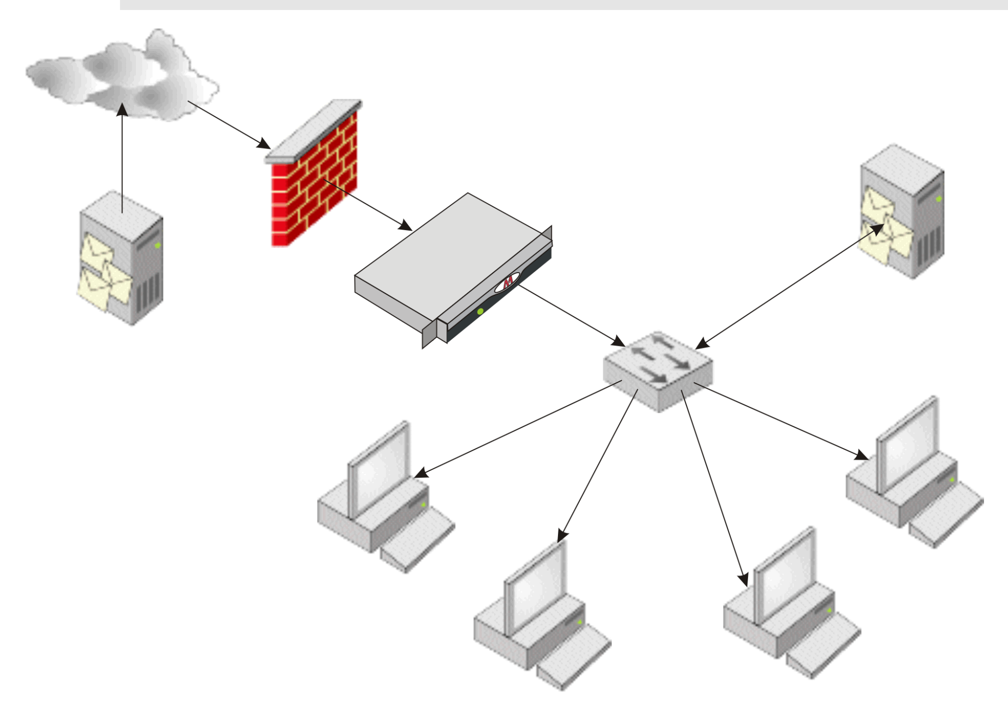


Abbildung 2-6 Netzwerkstruktur – Modus "Transparente Bridge"

Sie müssen wie folgt vorgehen:

- Konfigurieren Sie die Client-Geräte so, dass sie auf das Standard-Gateway verweisen.
- Konfigurieren Sie das Gerät so, dass das Internet-Gateway als Standard-Gateway verwendet wird.
- Stellen Sie sicher, dass Ihre Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.

Netzwerkkonfiguration für VMware vSphere

Diese Gruppe von Aufgaben stellt dar, wie Sie Ihre vSwitch-Konfiguration für die möglichen Betriebsmodi vorbereiten.

Vorgehensweise – Konfigurieren von VMware vSphere für eine Installation im Modus "Expliziter Proxy"

Gehen Sie wie nachfolgend beschrieben vor, um VMware vSphere so zu konfigurieren, dass die virtuelle Appliance im Modus "Expliziter Proxy"installiert wird.

Bevor Sie beginnen

Stellen Sie sicher, dass auf Ihrem VMware ESX-Host mindestens zwei verschiedene physische Schnittstellen zur Verfügung stehen. Eine dritte Schnittstelle kann für die Out-of-band-Verwaltung verwendet werden.

Aus Gründen der Leistungsoptimierung empfiehlt McAfee, die von der virtuellen Maschine mit McAfee Email Gateway Virtual Appliance verwendeten Schnittstellen nicht von anderen virtuellen Maschinen auf diesem VMware ESX-Host nutzen zu lassen. Bevor Sie mit der Installation der virtuellen Appliance beginnen, müssen vSwitches erstellt worden sein, die mit LAN 1 und LAN 2 der virtuellen Appliance verbunden werden können und die ordnungsgemäß konfiguriert sind.

Wenn Sie die .OVA-Datei für McAfee Email Gateway Virtual Appliance importieren, stellen Sie sicher, dass die **LAN**-**1**-Schnittstelle mit dem ersten vSwitch und die **LAN**-**2**-Schnittstelle mit dem zweiten vSwitch verbunden ist.



Sie müssen auf jedem Host im Hochverfügbarkeits-Cluster (High Availability, HA) identische vSwitches erstellen, falls VMotion eingesetzt wird.

Vorgehensweise

1. Melden Sie sich beim vSphere Client an.
2. Wählen Sie im linken Bereich der Ansicht **Hosts and Clusters** (Hosts und Cluster) den Host aus, auf dem Sie die virtuelle Appliance installieren möchten.
3. Wählen Sie auf der rechten Seite **Configuration** (Konfiguration).
4. Klicken Sie auf **Networking** (Netzwerk).
5. Klicken Sie auf **Add Networking** (Netzwerk hinzufügen).
6. Wählen Sie im Assistenten **Add Network** (Netzwerk hinzufügen) **Virtual Machine** (Virtuelle Maschine) aus, und klicken Sie auf **Next** (Weiter).
7. Wählen Sie **Create a virtual switch** (Virtuellen Switch erstellen), wählen Sie die physische Schnittstelle aus, die Sie für die LAN-1-Verbindung der virtuellen Appliance verwenden möchten, und klicken Sie auf **Next** (Weiter).
8. Geben Sie eine Bezeichnung für Ihr neues Netzwerk ein, z. B. `MEG LAN 1`.
9. Klicken Sie auf **Next** (Weiter) und anschließend auf **Finish** (Fertig stellen).
10. Wiederholen Sie die Schritte 5 bis 10, um einen zweiten vSwitch für die LAN-2-Schnittstelle hinzuzufügen.

Vorgehensweise – Konfigurieren von VMware vSphere für eine Installation im Modus "Transparente Bridge"

Gehen Sie wie nachfolgend beschrieben vor, um VMware vSphere so zu konfigurieren, dass die virtuelle Appliance im Modus "Transparente Bridge" installiert wird.

Bevor Sie beginnen

Stellen Sie sicher, dass auf Ihrem VMware ESX-Host mindestens zwei verschiedene physische Schnittstellen zur Verfügung stehen. Die beiden Schnittstellen, die für die Bridge verwendet werden, müssen mit verschiedenen Broadcast-Domänen verbunden sein, um Netzwerk-Loops zu vermeiden, die schwerwiegende Störungen in Ihrem Netzwerk verursachen könnten. Eine dritte Schnittstelle kann für die Out-of-band-Verwaltung verwendet werden.

Aus Gründen der Leistungsoptimierung empfiehlt McAfee, die von der Bridge verwendeten Schnittstellen der virtuellen Maschine mit McAfee Email Gateway Virtual Appliance dediziert zuzuordnen und nicht von anderen virtuellen Maschinen auf diesem VMware ESX-Host

nutzen zu lassen. Bevor Sie mit der Installation der virtuellen Appliance beginnen, müssen vSwitches erstellt worden sein, die mit LAN 1 und LAN 2 der virtuellen Appliance verbunden werden können und die ordnungsgemäß konfiguriert sind.

Wenn Sie die .OVA-Datei für McAfee Email Gateway Virtual Appliance importieren, stellen Sie sicher, dass die **LAN-1**-Schnittstelle mit dem ersten vSwitch und die **LAN-2**-Schnittstelle mit dem zweiten vSwitch verbunden ist.



Sie müssen auf jedem Host im Hochverfügbarkeits-Cluster (High Availability, HA) identische vSwitches erstellen, falls VMotion eingesetzt wird.

Vorgehensweise

1. Melden Sie sich beim vSphere Client an.
2. Wählen Sie im linken Bereich der Ansicht **Hosts and Clusters** (Hosts und Cluster) den Host aus, auf dem Sie die virtuelle Appliance installieren möchten.
3. Wählen Sie auf der rechten Seite **Configuration** (Konfiguration).
4. Klicken Sie auf **Networking** (Netzwerk).
5. Klicken Sie auf **Add Networking** (Netzwerk hinzufügen).
6. Wählen Sie im Assistenten **Add Network** (Netzwerk hinzufügen) **Virtual Machine** (Virtuelle Maschine) aus, und klicken Sie auf **Next** (Weiter).
7. Wählen Sie **Create a virtual switch** (Virtuellen Switch erstellen), wählen Sie die physische Schnittstelle aus, die Sie für die LAN-1-Verbindung der virtuellen Appliance verwenden möchten, und klicken Sie auf **Next** (Weiter).
8. Geben Sie eine Bezeichnung für Ihr neues Netzwerk ein, z. B. `MEG LAN 1`.

   Standardmäßig entfernt VMware ESX VLAN-Tags. Damit die virtuelle Appliance den für das VLAN gekennzeichneten Datenverkehr sehen kann (beispielsweise für das Erstellen VLAN-spezifischer Richtlinien), müssen Sie **Virtual Guest Tagging** aktivieren. Weitere Informationen hierzu finden Sie im Artikel 1004252 der VMware Knowledge Base.

9. Klicken Sie auf **Next** (Weiter) und anschließend auf **Finish** (Fertig stellen).
10. Blättern Sie auf der Seite nach unten zu dem virtuellen Switch, den Sie gerade erstellt haben, und klicken Sie auf **Properties** (Eigenschaften).
11. Doppelklicken Sie in **vSwitch Properties** (vSwitch-Eigenschaften) links in der Liste auf den Eintrag **vSwitch**.
12. Klicken Sie auf **Security** (Sicherheit).
13. Ändern Sie den Wert im Feld **Promiscuous Mode** (Promiscuous-Modus) in **Accept** (Akzeptieren), und klicken Sie auf **OK**.
14. Klicken Sie auf **Schließen**.
15. Wiederholen Sie die Schritte 5 bis 14, um einen zweiten vSwitch für die LAN-2-Schnittstelle hinzuzufügen.

   Die zweite vSwitch muss mit einer anderen physischen Schnittstelle verbunden werden, die ihrerseits mit einer anderen Broadcast-Domäne in Ihrem Netzwerk verbunden sein muss, als es die für den ersten vSwitch verwendete Schnittstelle ist.

Vorgehensweise – Konfigurieren von VMware vSphere für eine Installation im Modus "Transparenter Router"

Gehen Sie wie nachfolgend beschrieben vor, um VMware vSphere so zu konfigurieren, dass die virtuelle Appliance im Modus "Transparenter Router" installiert wird.

Bevor Sie beginnen

Stellen Sie sicher, dass auf Ihrem VMware ESX-Host mindestens zwei verschiedene physische Schnittstellen zur Verfügung stehen. Eine dritte Schnittstelle kann für die Out-of-band-Verwaltung verwendet werden.

Aus Gründen der Leistungsoptimierung empfiehlt McAfee, die von der virtuellen Maschine mit McAfee Email Gateway Virtual Appliance verwendeten Schnittstellen nicht von anderen virtuellen Maschinen auf diesem VMware ESX-Host nutzen zu lassen. Bevor Sie mit der Installation der virtuellen Appliance beginnen, müssen vSwitches erstellt worden sein, die mit LAN 1 und LAN 2 der virtuellen Appliance verbunden werden können und die ordnungsgemäß konfiguriert sind.

Wenn Sie die .OVA-Datei für McAfee Email Gateway Virtual Appliance importieren, stellen Sie sicher, dass die **LAN-1**-Schnittstelle mit dem ersten vSwitch und die **LAN-2**-Schnittstelle mit dem zweiten vSwitch verbunden ist.



Sie müssen auf jedem Host im Hochverfügbarkeits-Cluster (High Availability, HA) identische vSwitches erstellen, falls VMotion eingesetzt wird.

Vorgehensweise

1. Melden Sie sich beim vSphere Client an.
2. Wählen Sie im linken Bereich der Ansicht **Hosts and Clusters** (Hosts und Cluster) den Host aus, auf dem Sie die virtuelle Appliance installieren möchten.
3. Wählen Sie auf der rechten Seite **Configuration** (Konfiguration).
4. Klicken Sie auf **Networking** (Netzwerk).
5. Klicken Sie auf **Add Networking** (Netzwerk hinzufügen).
6. Wählen Sie im Assistenten **Add Network** (Netzwerk hinzufügen) **Virtual Machine** (Virtuelle Maschine) aus, und klicken Sie auf **Next** (Weiter).
7. Wählen Sie **Create a virtual switch** (Virtuellen Switch erstellen), wählen Sie die physische Schnittstelle aus, die Sie für die LAN-1-Verbindung der virtuellen Appliance verwenden möchten, und klicken Sie auf **Next** (Weiter).
8. Geben Sie eine Bezeichnung für Ihr neues Netzwerk ein, z. B. `MEG LAN 1`.
9. Klicken Sie auf **Next** (Weiter) und anschließend auf **Finish** (Fertig stellen).
10. Wiederholen Sie die Schritte 5 bis 10, um einen zweiten vSwitch für die LAN-2-Schnittstelle hinzuzufügen.

    Der zweite vSwitch muss mit einer anderen als der für Ihren ersten vSwitch verwendeten physischen Schnittstelle verbunden werden.

Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ

Lernen Sie demilitarisierte Zonen in Ihrem Netzwerk kennen, und erfahren Sie, wie Sie diese zum Schutz Ihrer E-Mail-Server verwenden können.

Eine "demilitarisierte Zone" (Demilitarized Zone, DMZ) ist ein Netzwerk, das durch eine Firewall von allen anderen Netzwerken getrennt ist, auch vom Internet und anderen internen Netzwerken. Eine DMZ wird üblicherweise mit dem Ziel implementiert, den Zugriff auf Server zu sperren, die Internetdienste (beispielsweise E-Mail) zur Verfügung stellen.

Hacker verschaffen sich oft Zugriff auf Netzwerke, indem sie herausfinden, auf welchen TCP-/UDP-Ports Appliances Anfragen erwarten, und dann bekannte Schwachstellen in Appliances ausnutzen. Firewalls senken das Risiko solcher Exploits erheblich, indem sie den Zugriff auf bestimmte Ports auf bestimmten Servern steuern.

Das Gerät kann einfach zu einer DMZ-Konfiguration hinzugefügt werden. Die Art, wie Sie das Gerät in einer DMZ verwenden, hängt von den zu scannenden Protokollen ab.

SMTP-Konfiguration in einer DMZ

Erfahren Sie, wie Sie SMTP-Geräte, die sich innerhalb einer demilitarisierten Zone Ihres Netzwerks befinden, konfigurieren.

Die DMZ ist eine gute Möglichkeit für das Verschlüsseln von E-Mails. Wenn der E-Mail-Verkehr die Firewall zum zweiten Mal erreicht (auf seinem Weg von der DMZ zum Internet), ist er verschlüsselt.

Geräte, die SMTP-Verkehr in einer DMZ scannen können, sind normalerweise im Modus "Expliziter Proxy" konfiguriert.

Konfigurationsänderungen müssen nur an den MX-Einträgen für die E-Mail-Server vorgenommen werden.



HINWEIS: Sie können den Modus "Transparente Bridge" verwenden, wenn Sie SMTP in einer DMZ scannen. Wenn Sie jedoch den Datenfluss nicht richtig steuern, scannt das Gerät jede Nachricht zweimal, einmal in jede Richtung. Aus diesem Grund wird für SMTP-Scans normalerweise der Modus "Expliziter Proxy" verwendet.

E-Mail-Relay

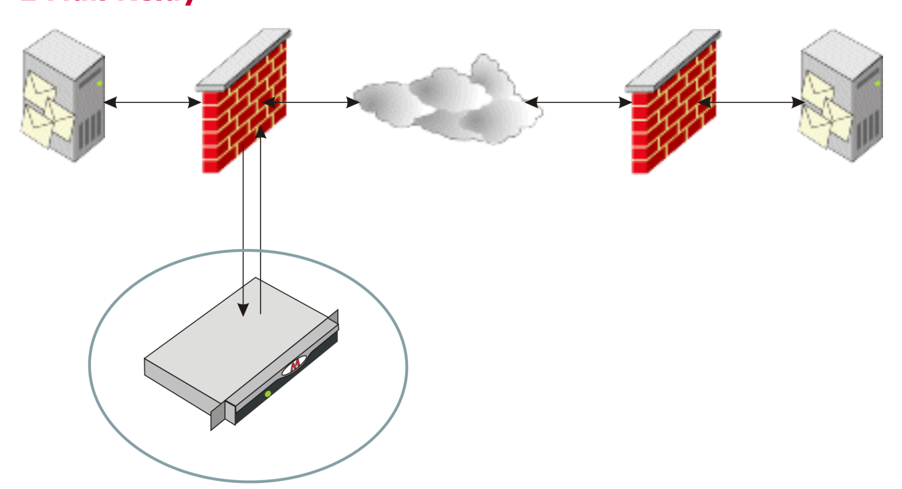


Abbildung 2-7 Konfigurieren als Mail-Relay

Wenn Sie in Ihrer DMZ bereits ein Relay eingerichtet haben, können Sie es durch das Gerät ersetzen.

Um Ihre bestehenden Firewall-Richtlinien zu verwenden, geben Sie dem Gerät dieselbe IP-Adresse wie dem Mail-Relay.

E-Mail-Gateway

SMTP bietet keine Methoden zur Verschlüsselung von E-Mail-Nachrichten. Sie können mithilfe von TLS (Transport Layer Security) den Link verschlüsseln, nicht jedoch die E-Mail-Nachrichten. Daher erlauben einige Unternehmen solchen Datenverkehr nicht in ihrem internen Netzwerk. Zur Umgehung dieses Problems wird häufig ein proprietäres E-Mail-Gateway eingesetzt, zum Beispiel Lotus Notes® oder Microsoft® Exchange, um den E-Mail-Datenverkehr zu verschlüsseln, bevor er das Internet erreicht.

Um eine DMZ-Konfiguration unter Verwendung des proprietären E-Mail-Gateways zu implementieren, fügen Sie das Scan-Gerät zur DMZ auf der SMTP-Seite des Gateways hinzu.

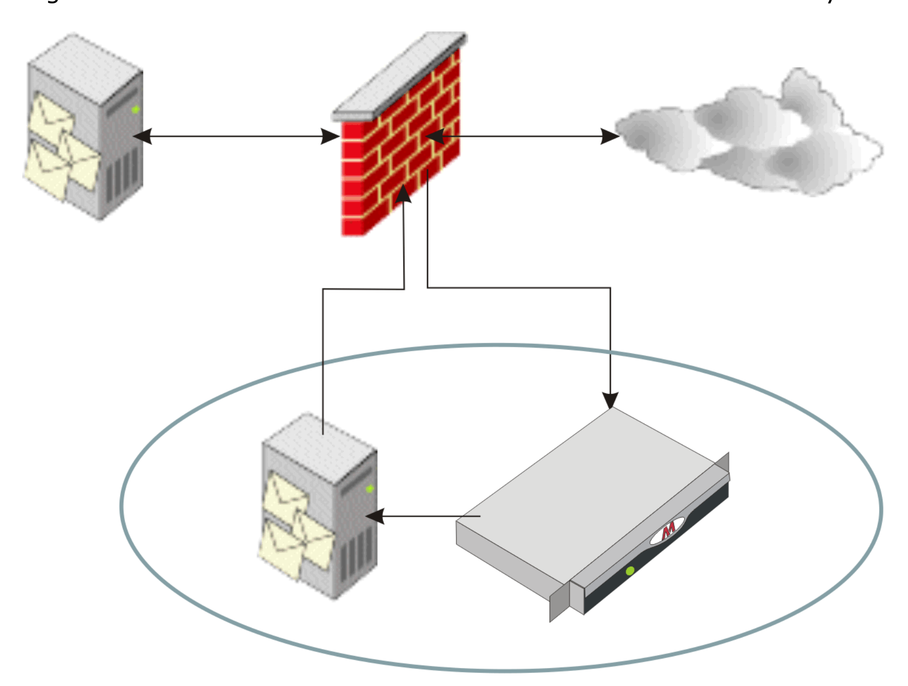


Abbildung 2-8 Konfigurieren als E-Mail-Gateway

Nehmen Sie hierfür folgende Konfigurationen vor:

- Die öffentlichen MX-Einträge müssen externe Mail-Server anweisen, alle eingehenden E-Mail-Nachrichten an das Gerät (statt an das Gateway) zu senden.
- Das Gerät muss alle eingehenden E-Mail-Nachrichten an das Mail-Gateway und alle ausgehenden Nachrichten per DNS oder über ein externes Relay senden.
- Das E-Mail-Gateway muss alle eingehenden E-Mails an die internen Mail-Server und aller andere (ausgehenden) Mails an das Gerät weiterleiten.
- Die Firewall erlaubt nur eingehende E-Mails, die sich an das Gerät richten.



Bei Firewalls, auf denen die Verwendung von NAT (Network Address Translation) konfiguriert ist und die eingehende E-Mails an die internen E-Mail-Server umleiten, müssen die öffentlichen MX-Einträge nicht neu konfiguriert werden. Sie leiten den Datenverkehr bereits an die Firewall und nicht an das eigentliche E-Mail-Gateway. In diesem Fall muss die Firewall neu konfiguriert werden, sodass eingehende Nachrichten an das Gerät geleitet werden.

Systemanforderungen

Stellen Sie mithilfe dieser Informationen sicher, dass Ihr Host-Computer die Systemanforderungen für die von Ihnen gewählte virtuelle VMware-Umgebung erfüllt.



Lesen Sie den VMware Knowledge Base-Artikel 1003661 unter http://www.vmware.com, um sich über die Mindestanforderungen an Ihr System für VMware ESX oder VMware ESXi 4.x zu informieren. Sie benötigen einen Computer mit einer 64-Bit-x86-CPU.

Darüber hinaus müssen Sie sicherstellen, dass die verwendete virtuelle Maschine die folgenden minimalen Systemanforderungen erfüllt:

Element	Spezifikation
Prozessor	Zwei virtuelle Prozessoren
Verfügbarer virtueller Speicher	2 GB
Freier Festplattenspeicher	80 GB



Wenn Sie planen, die McAfee Email Gateway Virtual Appliance im Modus "Transparente Bridge" zu installieren, benötigen Sie auf dem physischen VMware ESX-Host zwei externe Netzwerkschnittstellen, die mit verschiedenen Broadcast-Domänen verbunden sind. Aus Gründen der Leistungsoptimierung empfiehlt McAfee, diese beiden Schnittstellen nicht von anderen virtuellen Maschinen auf diesem physischen Host nutzen zu lassen. Wenn die beiden Schnittstellen einer Bridge mit derselben Broadcast-Domäne verbunden werden, entsteht in Ihrem Netzwerk eine STP-Schleife, die Netzwerkausfälle verursachen kann.

Beispiel-Installationsszenarien

In diesem Abschnitt enthalten Sie Informationen zur Installation der virtuellen Appliance in unterschiedlichen Server-Konfigurationen.

Ausführen der virtuellen Appliance als einzige virtuelle Maschine auf dem Host

Eine mögliche Ausbringung der virtuellen Appliance auf einem einzelnen Server in der von Ihnen gewählten virtuellen VMware-Umgebung.

VMware vSphere oder VMware vSphere Hypervisor sind dedizierte Server für die virtuelle Appliance. Deren Hardware-Spezifikation muss die minimalen Hardware-Anforderungen erfüllen, die in den *Richtlinien zu den McAfee Email Gateway-Leistungsdaten* dargelegt sind.



In diesem Beispiel wird davon ausgegangen, dass Sie die virtuelle Appliance im empfohlenen Modus "Expliziter Proxy" betreiben.

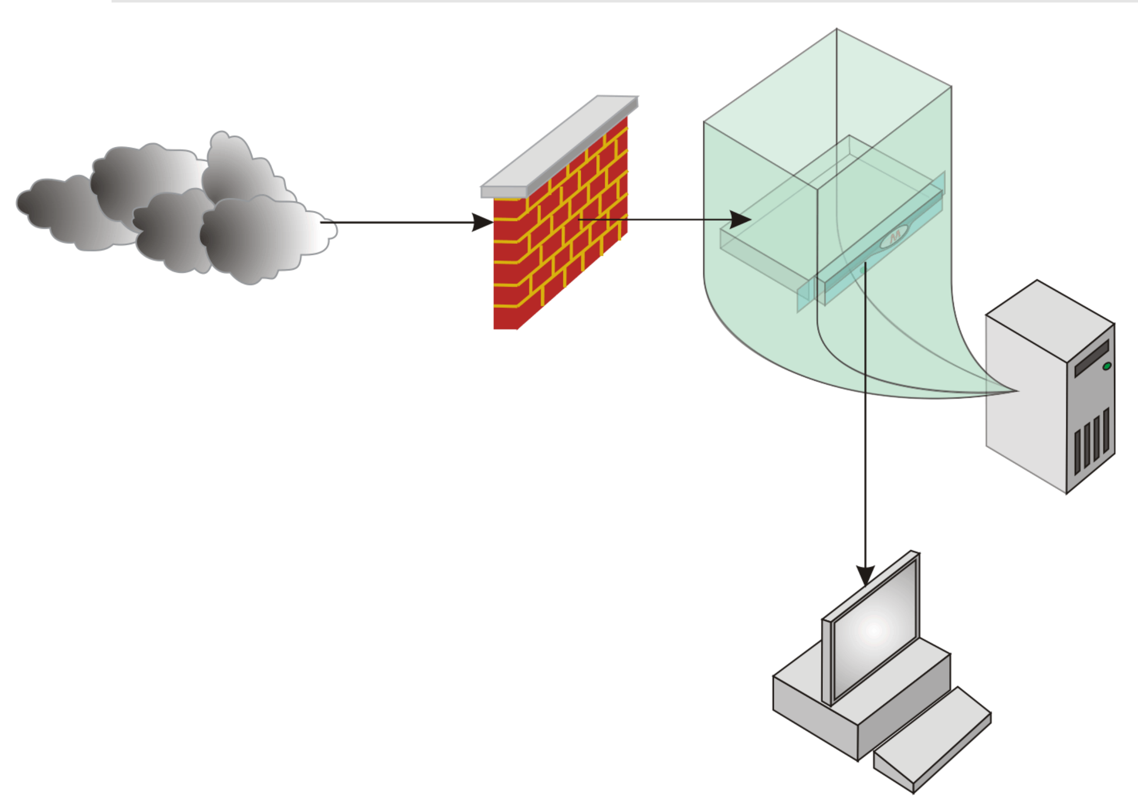


Abbildung 2-9 Ausbringung auf nur einem Server

Ausführen der virtuellen Appliance zusammen mit anderen virtuellen Maschinen

Eine mögliche Ausbringung von McAfee Email Gateway Virtual Appliance in Ihrer ausgewählten virtuellen Umgebung zusammen mit anderen virtuellen Maschinen.

In diesem Beispiel ist ein VMware-Host für die virtuelle Appliance sowie auch für andere virtuelle Maschinen verantwortlich, die alle auf derselben Hardware ausgeführt werden. Auf der VMware-Website http://www.vmware.com finden Sie Informationen zum Aufbau eines

Ressourcen-Pools für die virtuelle Appliance. Dem Ressourcen-Pool müssen außerdem die Mindestanforderungen an CPU und Arbeitsspeicher zugewiesen sein, wie sie in den *Richtlinien zu den McAfee Email Gateway-Leistungsdaten* dargelegt sind.



In diesem Beispiel wird davon ausgegangen, dass Sie die virtuelle Appliance im empfohlenen Modus "Expliziter Proxy" betreiben.

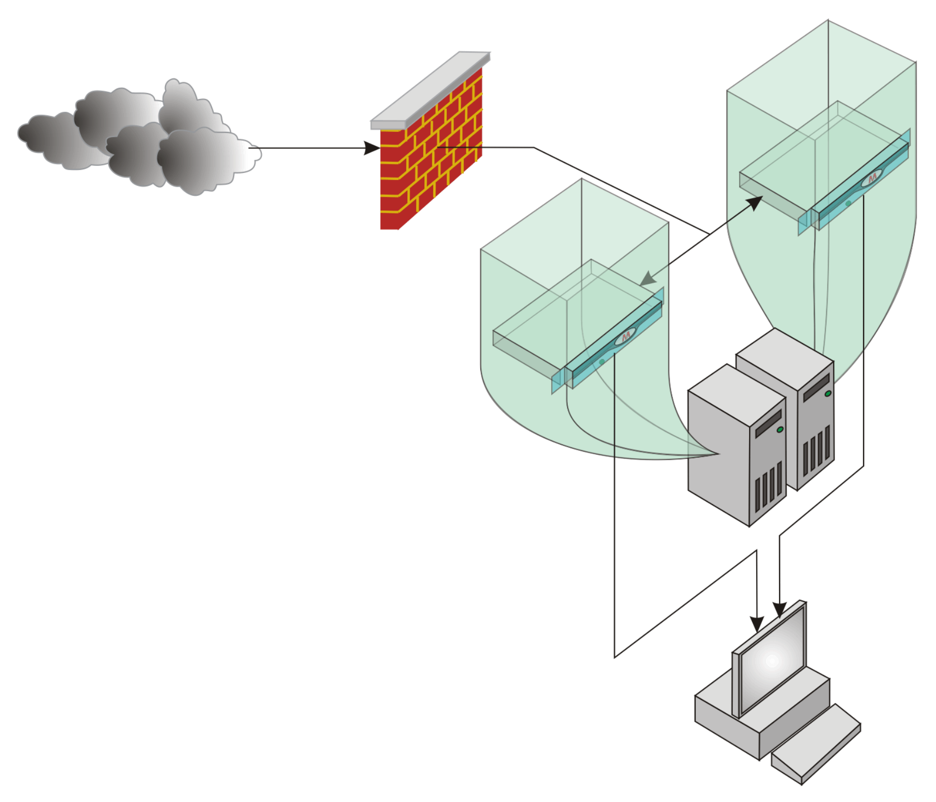


Abbildung 2-10 Ausbringung auf mehreren Servern

3 Installieren der McAfee Email Gateway Virtual Appliance

Diese Informationen unterstützen Sie bei der Einrichtung der virtuellen Umgebung und der Installation von McAfee Email Gateway Virtual Appliance.

Inhalt

Übersicht über den Installationsvorgang der virtuellen Appliance

In diesem Abschnitt erhalten Sie einen kurzen Überblick über die Schritte, die zur Installation der virtuellen Appliance erforderlich sind.

McAfee empfiehlt, dass Sie die virtuelle Appliance in der folgenden Reihenfolge installieren:

1. Installieren Sie das gewünschte VMware-Produkt.
2. Laden Sie die Installationsdateien der virtuellen Appliance herunter.
3. Installieren Sie die virtuelle Appliance in der virtuellen Umgebung.
4. Führen Sie die Konfiguration mithilfe des grafischen Konfigurationsassistenten durch.
5. Melden Sie sich an der virtuellen Appliance an.

6 Testen Sie die Konfiguration.

7 Aktivieren Sie Protokolle.

Bewährte Vorgehensweisen für die Installation

Diese Informationen geben Ihnen einige wichtige Anhaltspunkte für die Installation auf VMware vSphere.



McAfee empfiehlt, dass Sie diese Informationen lesen und danach handeln, bevor Sie mit der Installation beginnen.

- Die virtuelle Appliance ist am einfachsten einzurichten und zu warten, wenn sie im standardmäßigen Betriebsmodus "Expliziter Proxy" betrieben wird.
- Machen Sie sich mit den Informationen zum Erstellen von Clustern und Ressourcen-Pools vertraut. Siehe die VMware-Website http://www.vmware.com.
- Verwenden Sie ein Storage Area Network (SAN) statt eines Network File System (NFS), um optimale Ergebnisse zu erzielen.
- Wenn Sie die virtuelle Appliance in einem der transparenten Modi betreiben:
  - Die Funktionen VMware Distributed Resource Scheduler (DRS) und High Availability (HA) könnnen zu Netzwerkunterbrechungen führen, wenn ein Failover stattfindet.
  - Stellen Sie sicher, dass die Netzwerkkarten der virtuellen Appliance nicht mit derselben Broadcast-Domäne verbunden sind und dass sich die IP-Adressen nicht in demselben Subnetz befinden, um Netzwerk-Loops zu vermeiden.
  - Stellen Sie sicher, dass jeder Netzwerkadapter auf der virtuellen Appliance mit einem anderen physischen Netzwerk auf dem Host-Computer verbunden ist.
  - Sie benötigen mindestens drei Netzwerkkarten im VMware-Host. Die virtuelle Appliance benötigt zwei Netzwerkkarten. VMware empfiehlt, eine dedizierte Netzwerkkarte für die Service-Konsole zu verwenden.

Vorgehensweise – Konvertieren einer VMtrial-Installation

Migrieren Sie anhand dieser Vorgehensweise beliebige Konfigurationseinstellungen von einer McAfee Email Gateway Appliance (VMtrial)-Installation auf die McAfee Email Gateway Virtual Appliance.

Vorgehensweise

1 Wählen Sie in Ihrer VMtrial-Installation **System** | **Systemverwaltung** | **Konfigurationsverwaltung**.

2 Klicken Sie auf **Konfiguration sichern**, um die Konfigurationsdetails zu speichern.

3 Installieren Sie die McAfee Email Gateway Virtual Appliance-Software in der von Ihnen gewählten virtuellen Umgebung.

4 Melden Sie sich an, und öffnen Sie die McAfee Email Gateway Virtual Appliance-Software.

5 Wählen Sie **System** | **Systemverwaltung** | **Konfigurationsverwaltung**, und klicken Sie auf **Aus Datei wiederherstellen**.



Der Zugriff auf die Optionen zur Konfigurationswiederherstellung ist auch über **System** | **Setup-Assistent** möglich.

6 Gehen Sie zurück zur VMtrial-Konfigurationsdatei, die Sie wiederherstellen möchten, und klicken Sie auf **Öffnen**.

7 Wählen Sie die Teile der Datei aus, die Sie wiederherstellen möchten, und klicken Sie auf **OK**.

8 Überprüfen Sie, ob die Einstellungen erfolgreich importiert wurden, und übernehmen Sie die Änderungen.

Vorgehensweise – Herunterladen der Installations-Software

Gehen Sie wie nachfolgend beschrieben vor, um die aktuellste Version der McAfee Email Gateway-Software herunterzuladen.

Bevor Sie beginnen

- Lesen Sie das Installationshandbuch zu Ihrem -Produkt.
- Suchen Sie nach der McAfee-Grant-Nummer, die Sie beim Kauf von McAfee Email Gateway erhalten haben.

McAfee bietet die Software für die Installation in virtuellen Umgebungen als OVA-Datei an.

Vorgehensweise

1 Besuchen Sie die McAfee-Website http://www.mcafee.com. Halten Sie den Mauszeiger über Ihren Geschäftstyp, und klicken Sie auf **Downloads**.

2 Klicken Sie auf der Seite **Meine Produkte – Downloads** auf **Anmelden**.

3 Geben Sie die McAfee-Grant-Nummer ein, die Sie beim Kauf von McAfee Email Gateway erhalten haben, und klicken Sie auf **Senden**.

4 Wählen Sie aus der Produktliste **Email Gateway** aus.

5 Akzeptieren Sie die Lizenzbedingungen, wählen Sie die neueste Version, und laden Sie sie herunter.



McAfee empfiehlt, dass Sie die Versionsinformationen lesen, die Sie mit dem Software-Image erhalten, bevor Sie die Installation fortsetzen.

Vorgehensweise – Installation der Appliance auf VMware vSphere

Installieren Sie McAfee Email Gateway Virtual Appliance anhand dieser Vorgehensweise auf einem Host-Computer, auf dem VMware vSphere 4 oder VMware vSphere Hypervisor (ESXi) 4.0 ausgeführt wird.

Bevor Sie beginnen

- Stellen Sie sicher, dass die VMware vSphere-Konfiguration die Arbeit mit dem gewählten Betriebsmodus ermöglicht.
- Laden Sie das Paket für die McAfee Email Gateway Virtual Appliance von der McAfee-Download-Webseite herunter, und extrahieren Sie sie an einen Speicherort, auf den der VMware vSphere Client zugreifen kann.
- Installieren Sie eine lizenzierte Vollversion von VMware vSphere 4 oder VMware vSphere Hypervisor (ESXi) 4.

Wenn Sie das Produkt VMtrial verwendet haben, um die Software zu testen, können Sie Ihre VMtrial-Konfiguration speichern und im Anschuss an die Installation auf der virtuellen Appliance wiederherstellen.

Vorgehensweise

1. Starten Sie die VMware vSphere Client-Anwendung.
2. Melden Sie sich beim VMware vSphere-Server oder dem vCenter Server an.
3. Wählen Sie aus der Liste **Inventory** (Inventar) den Host oder Cluster, auf dem Sie die Software der virtuelle Appliance importieren möchten.
4. Klicken Sie auf **File | Deploy OVF Template | Deploy From File** (Datei | OVF-Vorlage bereitstellen | Aus Datei bereitstellen), klicken Sie auf **Durchsuchen**, und navigieren Sie zu dem Speicherort, an dem Sie die .OVA-Datei heruntergeladen haben.
5. Wählen Sie die Datei **McAfee-MEG-7.x-<build_number>.VMbuy.ova**, und klicken Sie auf **Öffnen**.
6. Klicken Sie zwei Mal auf **Next** (Weiter), und geben Sie optional einen neuen Namen ein.
7. Wählen Sie einen Ressourcen-Pool aus, sofern Sie einen konfiguriert haben.
8. Wählen Sie den Datenspeicher aus, und klicken Sie auf **Next** (Weiter).
9. Wählen Sie die virtuellen Netzwerke aus, mit denen die Netzwerkkarten der virtuellen Appliances verbunden werden.
10. Legen Sie die Größe der Festplatte für das Speichern von Daten fest, um den Speicherplatz zu erhöhen, der für isolierte, zurückgestellte und protokollierte Elemente reserviert wird.

    Für die Festplattengröße kann kein Wert definiert werden, der unterhalb der Standardgröße von 40 GB liegt.

11. Klicken Sie auf **Next** (Weiter), lesen Sie die Zusammenfassung, klicken Sie anschließend auf **Finish** (Fertig stellen), und warten Sie, bis der Importvorgang beendet ist.

Vorgehensweise – Verbessern der Systemleistung auf VMware vSphere

Mithilfe der folgenden Schritte können Sie möglicherweise die Systemleistung in VMware vSphere-Umgebungen steigern, indem Sie die Standardeinstellungen für Festplatten, Netzwerkadapter, Arbeitsspeicher und CPU ändern.

Vorgehensweise

1. So bearbeiten Sie die Festplatteneinstellungen:
   a. Prüfen Sie, ob die virtuelle Maschine ausgeschaltet ist.
   b. Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance in der Liste **Inventory** (Inventar), und klicken Sie auf **Edit Settings** (Einstellungen bearbeiten).

Im Dialogfeld **Virtual Machine Properties** (Eigenschaften der virtuellen Maschine) befinden sich drei Festplatten, die der virtuellen Appliance zur Verfügung stehen:

- **Hard disk 1** (Festplatte 1) enthält die Installationsdateien der virtuellen Appliance und darf weder entfernt noch verändert werden.
- **Hard disk 2** (Festplatte 2) ist die Hauptfestplatte, die von der virtuellen Appliance verwendet wird. Sie können deren Größe verändern, McAfee empfiehlt jedoch, sie nicht zu verkleinern.
- **Hard disk 3** (Festplatte 3) enthält den temporären Swap-Speicher der virtuellen Appliance.



Die Leistung kann möglicherweise erhöht werden, indem die zweite und die dritte Festplatte auf zwei getrennten Datenspeichern abgelegt werden.

2. So bearbeiten Sie die Einstellungen für Arbeitsspeicher und virtuelle CPU:
   - Prüfen Sie, ob die virtuelle Maschine ausgeschaltet ist.
   - Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance in der Liste "Inventory" (Inventar), und klicken Sie auf **Edit Settings** (Einstellungen bearbeiten).
   - Ändern Sie im Dialogfeld **Virtual Machine Properties** (Eigenschaften der virtuellen Maschine) die Einstellungen nach Bedarf.



McAfee empfiehlt, dass Sie die Einstellungen nicht auf weniger als die Standardeinstellungen oder die empfohlenen Systemanforderungen für die virtuelle Appliance herabsetzen.

Nach der Installation der Appliance kann die Größe der Festplatte nicht mehr verändert werden.

Konfiguration der virtuellen Appliance

Gehen Sie wie nachfolgend beschrieben vor, um die virtuelle Appliance zu konfigurieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihre virtuelle Umgebung installiert ist und ordnungsgemäß ausgeführt wird.

Vorgehensweise

1. Starten Sie die virtuelle Appliance. Die Installation beginnt automatisch.
2. Lesen Sie die Endbenutzer-Lizenzvereinbarung, um die Installation fortzusetzen, und klicken Sie dann auf **j**, um sie zu akzeptieren und mit der Installation zu beginnen.
3. Wählen Sie beim Installationsmenü **a** aus, um eine vollständige Installation auszuführen, und **j**, um fortzufahren.
4. Nachdem die Installation abgeschlossen ist, wird die virtuelle Appliance neu gestartet.
5. Wählen Sie im Eröffnungsfenster die Sprache aus, die Sie verwenden möchten.
6. Stimmen Sie den Bedingungen des Lizenzvertrags zu.
7. Konfigurieren Sie die virtuelle Appliance mithilfe des grafischen Konfigurationsassistenten.
8. Übernehmen Sie die Konfiguration auf die virtuelle Appliance. In Abhängigkeit von den eingegebenen Einstellungen wird möglicherweise ein Neustart durchgeführt. Sie können die

virtuelle Appliance auf mehr als einem VMware vSphere-, VMware vSphere Hypervisor- oder VMware Player-Server installieren. Gehen Sie dazu folgendermaßen vor:

a Führen Sie die Schritte in dieser Aufgabe auf einem anderen VMware vSphere-, VMware vSphere Hypervisor- oder VMware Player-Server aus.

b Kehren Sie zur Benutzeroberfläche der zuvor installierten virtuelle Appliance zurück.

c Wählen Sie **System** | **Systemverwaltung** | **Konfigurations-Push**, um die Konfigurationsdetails an die zweite virtuelle Appliance zu senden.

Verwenden der Konfigurationskonsole

Erfahren Sie, wie Sie das McAfee Email Gateway mithilfe der Konfigurationskonsole einrichten.

Sie können Ihr McAfee Email Gateway entweder von der Konfigurationskonsole aus oder innerhalb der Benutzeroberfläche mit dem Setup-Assistenten konfigurieren.

Die Konfigurationskonsole wird am Ende der Startsequenz automatisch gestartet, entweder nachdem:

- ein nicht konfiguriertes McAfee Email Gateway gestartet wurde,
- oder nachdem ein McAfee Email Gateway auf die Werkseinstellungen zurückgesetzt wurde.

Nach dem Start bietet Ihnen die **Konfigurationskonsole** Optionen, um Ihr Gerät von der McAfee Email Gateway-Konsole aus in Ihrer bevorzugten Sprache zu konfigurieren, bzw. liefert Anweisungen dafür, wie Sie von einem anderen Computer im selben Klasse-C-Subnetz (/24) aus eine Verbindung mit dem **Setup-Assistenten** innerhalb der Benutzeroberfläche herstellen können. Beide Methoden bieten Ihnen dieselben Optionen für die Konfiguration Ihres McAfee Email Gateway.



Von der **Konfigurationskonsole** aus können Sie eine neue Installation der Appliance-Software konfigurieren. Wenn Sie jedoch für die Konfiguration Ihrer Appliance eine zuvor gespeicherte Konfigurationsdatei verwenden möchten, müssen Sie sich bei der Benutzeroberfläche der Appliance anmelden und den Setup-Assistenten ausführen (**System | Setup-Assistent**).

Ebenso wird mit dieser Softwareversion für folgende Parameter die automatische Konfiguration mithilfe von DHCP eingeführt:

- Host-Name
- Domänenname
- Standard-Gateway
- DNS-Server
- Geleaste IP-Adresse
- NTP-Server

Weitere Informationen zu jeder Seite der **Konfigurationskonsole** und des **Setup-Assistenten** erhalten Sie auf dem Bildschirm.

Durchführen der Standardeinrichtung

In diesem Abschnitt erfahren Sie, welchen Zweck die Standardeinrichtung hat.

Die **Standardeinrichtung** ermöglicht Ihnen die schnelle Einrichtung Ihres McAfee Email Gateways unter Verwendung der gängigsten Optionen. Verwenden Sie diese Option, um das Gerät im Modus "Transparente Bridge" einzurichten und für den Schutz Ihres Netzwerks zu konfigurieren. Das SMTP-Protokoll ist standardmäßig aktiviert. Sie können wählen, ob POP3-Verkehr gescannt werden soll.



Mit der Wahl der **Standardeinrichtung** wird für das Gerät der Modus "Transparente Bridge" erzwungen.

Bei der **Standardeinrichtung** enthält der Assistent die folgenden Seiten:

- **E-Mail-Konfiguration**
- **Grundlegende Einstellungen**
- **Zusammenfassung**

Durchführen der benutzerdefinierten Einrichtung

In diesem Abschnitt erfahren Sie, welchen Zweck die benutzerdefinierte Einrichtung hat.

Die **Benutzerdefinierte Einrichtung** ermöglicht Ihnen eine größere Kontrolle über die Optionen, die Sie auswählen können, darunter den Betriebsmodus des Geräts. Sie können auswählen, dass der E-Mail-Verkehr über die Protokolle SMTP und POP3 geschützt wird. Verwenden Sie diese Konfigurationsoption, um IPv6 zu konfigurieren und sonstige Änderungen an der Standardkonfiguration vorzunehmen.

Bei der **Benutzerdefinierten Einrichtung** enthält der Assistent die folgenden Seiten:

- **E-Mail-Konfiguration**
- **Grundlegende Einstellungen**
- **Netzwerkeinstellungen**
- **Cluster-Verwaltung**
- **DNS und Routing**
- **Zeiteinstellungen**
- **Kennwort**
- **Zusammenfassung**

Wiederherstellung aus einer Datei

In diesem Abschnitt erfahren Sie, welchen Zweck die Wiederherstellung aus einer Datei hat.

Wenn Sie Ihr Gerät über den **Setup-Assistenten** innerhalb der Benutzeroberfläche konfigurieren, können Sie mithilfe der Option **Aus Datei wiederherstellen** zuvor gespeicherte Konfigurationsdaten importieren und auf Ihr Gerät übernehmen. Nachdem diese Daten importiert wurden, können Sie Änderungen vornehmen, bevor Sie die Konfiguration anwenden.



Die Option **Aus Datei wiederherstellen** ist in der **Konfigurationskonsole** nicht verfügbar. Zum Verwenden dieser Option müssen Sie sich beim McAfee Email Gateway anmelden und **Aus Datei wiederherstellen** aus dem Menü **System | Setup-Assistent** auswählen.

Nachdem die Konfigurationsdaten importiert wurden, werden die Optionen der **Benutzerdefinierten Einrichtung** im **Setup-Assistenten** angezeigt (siehe *Durchführen der benutzerdefinierten Einrichtung*). Alle importierten Optionen werden auf den Assistentenseiten angezeigt, sodass Sie die Möglichkeit zum Vornehmen von Änderungen haben, bevor Sie die Konfiguration übernehmen.

Bei Verwendung der Option **Aus Datei wiederherstellen** enthält der Assistent die folgenden Seiten:

- **Konfigurationsdatei importieren**
- **Wiederherzustellende Werte**

Nachdem diese Informationen geladen wurden, werden die Seiten der **Benutzerdefinierten Einrichtung** angezeigt, in denen Sie weitere Änderungen vornehmen können, bevor Sie die neue Konfiguration übernehmen:

- **E-Mail-Konfiguration**
- **Grundlegende Einstellungen**
- **DNS und Routing**
- **Zeiteinstellungen**

- **Netzwerkeinstellungen**
- **Cluster-Verwaltung**
- **Kennwort**
- **Zusammenfassung**

Einrichten der Verwaltung durch ePolicy Orchestrator

In diesem Abschnitt erfahren Sie, welchen Zweck die Option **Einrichten der Verwaltung durch ePolicy Orchestrator** hat.

McAfee ePolicy Orchestrator ermöglicht Ihnen, Ihre gesamten McAfee®-Software- und Hardware-Appliances von einer einzelnen Verwaltungskonsole aus zu verwalten.

Mit dem Assistenten **Einrichten der Verwaltung durch ePolicy Orchestrator** können Sie Ihr Gerät so konfigurieren, dass es von Ihrem McAfee ePolicy Orchestrator-Server aus verwaltet werden kann.

Es wird nur ein Minimum an Informationen benötigt, da das Gerät die meisten Konfigurationsdaten von Ihrem McAfee ePolicy Orchestrator-Server erhält.

Einstellungen für die ePolicy Orchestrator-Verwaltung

Wählen Sie „Einrichten der Verwaltung durch ePolicy Orchestrator" im Setup-Assistenten, um die Appliance für die Verwaltung durch McAfee ePolicy Orchestrator zu konfigurieren.

Option	Beschreibung
ePO-Erweiterungen	Laden Sie die McAfee ePolicy Orchestrator-Erweiterungen für McAfee Gateway-Produkte herunter, einschließlich McAfee Email Gateway. Die Datei *MEGv7.x_ePOextensions.zip* enthält sowohl die EWG- als auch die MEG McAfee ePolicy Orchestrator-Erweiterungen. Die EWG-Erweiterung ermöglicht die Berichterstellung von McAfee ePolicy Orchestrator aus für die folgenden Produkte: • McAfee Email and Web Security-Appliances • McAfee Web Gateway-Appliances • McAfee E-Mail Gateway-Appliances Die MEG-Erweiterung bietet eine vollständige McAfee ePolicy Orchestrator-Verwaltung für McAfee Email Gateway Versionen 7.0 oder höher. Damit Sie McAfee ePolicy Orchestrator für die Berichterstellung oder Verwaltung verwenden können, müssen die McAfee ePolicy Orchestrator-Erweiterungen auf Ihrem McAfee ePolicy Orchestrator-Server installiert sein.
ePO-Hilfe-Erweiterungen	Laden Sie die McAfee ePolicy Orchestrator-Hilfe-Erweiterungen herunter. Die Datei *MEGv7.x_ePOhelpextensions.zip* enthält die Informationen zur Online-Hilfe für die obigen McAfee ePolicy Orchestrator-Erweiterungen. Diese Datei installiert die zu den McAfee ePolicy Orchestrator-Erweiterungen für McAfee Email and Web Gateway sowie McAfee Email Gateway Appliances gehörenden Hilfe-Erweiterungen auf Ihrem McAfee ePolicy Orchestrator-Server.
ePO-Verbindungseinstellungen importieren	Klicken Sie hier, um zur Datei mit den Verbindungseinstellungen für McAfee ePolicy Orchestrator zu navigieren und die McAfee ePolicy Orchestrator-Verbindungsinformationen in die Appliance zu importieren.

Vorgehensweise – Konfigurieren der Appliance für das Arbeiten mit ePolicy Orchestrator

Richten Sie anhand dieser Vorgehensweise die Appliance für die Verwaltung durch ePolicy Orchestrator ein:

1. Wählen Sie auf dem McAfee Email Gateway unter **Einstellungen für die ePO-Verwaltung** die Option **ePO-Erweiterungen**, und klicken Sie auf **Speichern**, um die Erweiterungsdatei herunterzuladen.
2. Wählen Sie auf dem McAfee Email Gateway unter **Einstellungen für die ePO-Verwaltung** die Option **ePO-Hilfe-Erweiterungen**, und klicken Sie auf **Speichern**, um die Hilfe-Erweiterungsdatei herunterzuladen.
3. Installieren Sie diese Erweiterungen auf Ihrem McAfee ePolicy Orchestrator-Server, indem Sie **Menü** | **Software** | **Erweiterungen** | **Erweiterungen installieren** wählen.
4. Speichern Sie auf dem McAfee ePolicy Orchestrator-Server die Verbindungseinstellungen mithilfe des Befehls **Menü** | **Gateway-Schutz** | **E-Mail- und Web-Gateway** | **Aktionen** | **Verbindungseinstellungen exportieren**.
5. Kehren Sie auf dem McAfee Email Gateway auf die Seite **Einstellungen für die ePO-Verwaltung** im **Setup-Assistenten** zurück, und klicken Sie auf **ePO-Verbindungseinstellungen importieren**. Navigieren Sie zur McAfee ePolicy Orchestrator-Verbindungseinstellungsdatei.
6. Klicken Sie auf **Weiter**, um auf der Seite **Grundlegende Einstellungen** im **Setup-Assistenten** fortzufahren.

Setup im Modus 'Nur Verschlüsselung'

In diesem Abschnitt erfahren Sie, welchen Zweck die Einrichtungsoptionen im Modus "Nur Verschlüsselung" haben.

In kleinen bis mittleren Organisationen ist es häufig ausreichend, dasselbe McAfee Email Gateway für E-Mail-Scan- und E-Mail-Verschlüsselungs-Tasks zu verwenden.

Wenn Sie jedoch in einem größeren Unternehmen bzw. in einer Branche arbeiten, in der die Zustellung des gesamten oder eines überwiegenden Teils des E-Mail-Aufkommens auf eine sichere Weise erfolgen muss, kann es empfehlenswert sein, eine oder mehrere McAfee Email Gateway Appliances als eigenständige Verschlüsselungs-Server einzurichten.

Unter diesen Umständen bieten Ihnen die Optionen für das **Setup im Modus "Nur Verschlüsselung"** innerhalb des **Setup-Assistenten** die relevanten Einstellungen, die für den Betrieb im Modus "Nur Verschlüsselung" erforderlich sind.

4 Vorstellung des Dashboards

In diesem Abschnitt wird die Seite **Dashboard** beschrieben und erläutert, wie ihre Voreinstellungen bearbeitet werden.

Das Dashboard

Das **Dashboard** bietet eine Zusammenfassung der Aktivitäten der Appliance.



Dashboard

Von dieser Seite aus können Sie auf die meisten Seiten zugreifen, die die Appliance steuern.

Auf einer Cluster-Master-Appliance verwenden Sie diese Seite auch, um eine Übersicht der Aktivitäten im Appliance-Cluster anzuzeigen.

Vorteile der Verwendung des Dashboards

Das **Dashboard** bietet einen zentralen Ort, an dem Sie Zusammenfassungen der Appliance-Aktivitäten mithilfe verschiedener Portlets ansehen können.

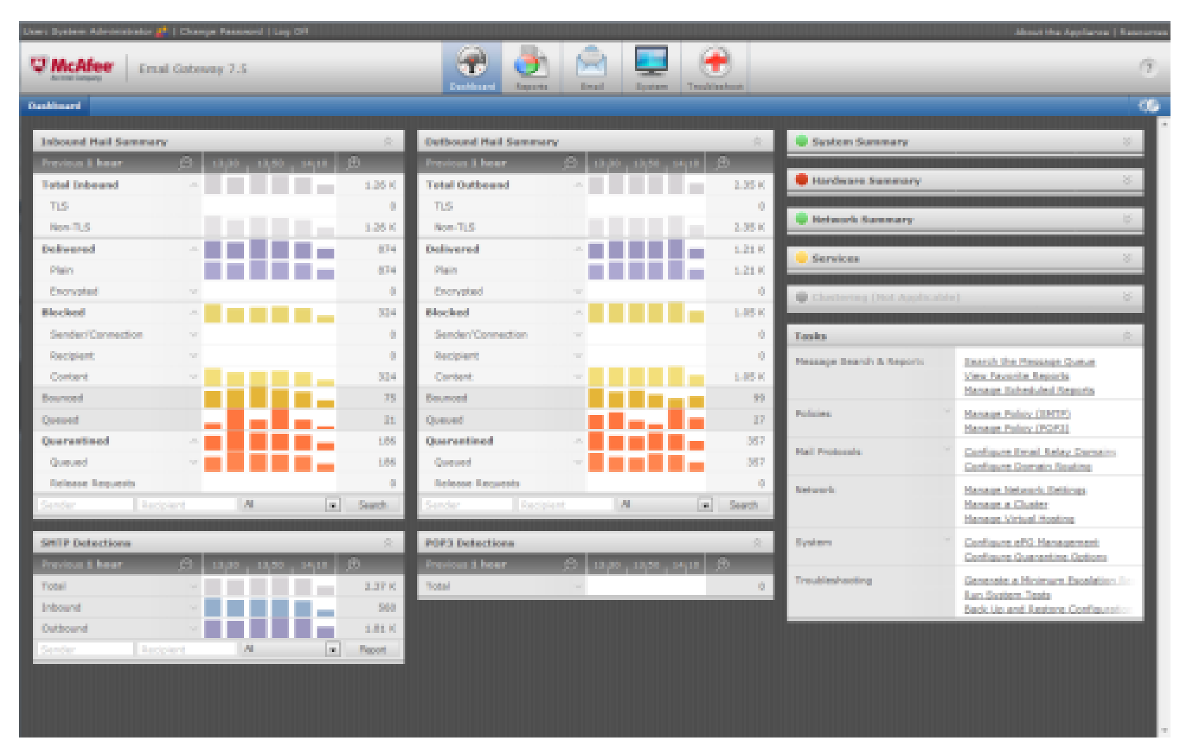


Abbildung 4-1 Dashboard-Portlets

In einigen Portlets werden Grafiken angezeigt, die die Appliance-Aktivität in den folgenden Zeiträumen darstellen:

- 1 Stunde
- 1 Tag (Standard)
- 1 Woche
- 2 Wochen
- 4 Wochen

Im **Dashboard** können Sie einige Änderungen an den angezeigten Informationen und Diagrammen vornehmen:

- Vergrößern und verkleinern Sie die Portlet-Daten mithilfe der Schaltflächen und rechts oben im Portlet.
- Zeigen Sie mithilfe der Schaltflächen und detailliertere Daten an.
- Eine Statusanzeige gibt an, ob das Element Aufmerksamkeit erfordert:
  - **Fehlerfrei**: Die ausgewiesenen Elemente funktionieren normal.
  - **Erfordert Aufmerksamkeit**: Ein Warnungsschwellenwert wurde überschritten.
  - **Erfordert sofortige Aufmerksamkeit**: Ein kritischer Schwellenwert wurde überschritten.
  - **Deaktiviert**: Der Dienst ist nicht aktiviert.

- Verwenden Sie und , um auf einer Zeitachse in Informationen herein- und herauszuzoomen. Es kommt zu einer kurzen Verzögerung, während die Ansicht aktualisiert wird. Standardmäßig zeigt das **Dashboard** Daten für den vorherigen Tag an.
- Verschieben Sie ein Portlet an eine andere Stelle auf dem **Dashboard**.
- Doppelklicken Sie auf die obere Leiste eines Portlets, um es auf den oberen Bereich des **Dashboards** zu vergrößern.
- Legen Sie eigene Warnhinweis- und Warnungsschwellenwerte zum Auslösen von Ereignissen fest. Markieren Sie dazu das Element, und klicken Sie darauf, bearbeiten Sie die Felder "Warnhinweisschwellenwert" und "Warnungsschwellenwert", und klicken Sie auf **Speichern**. Wenn das Element den von Ihnen festgelegten Schwellenwert überschreitet, wird ein Ereignis ausgelöst.



Abhängig von dem Browser, der zum Anzeigen der Benutzeroberfläche von McAfee Email Gateway verwendet wird, speichert das **Dashboard** den aktuellen Status jedes Portlets (ob es vergrößert oder verkleinert ist und ob Sie die Anzeige bestimmter Daten geöffnet haben) und versucht, die entsprechende Ansicht wiederherzustellen, wenn Sie zu einer anderen Seite in der Benutzeroberfläche navigieren und anschließend innerhalb derselben Browsersitzung zum **Dashboard** zurückkehren.

Dashboard-Portlets

Lernen Sie die Portlets auf dem Dashboard der Benutzeroberfläche von McAfee Email Gateway kennen.

Option	Beschreibung
Zusammenfassung der eingehenden E-Mails	Mit dem Portlet **Zusammenfassung der eingehenden E-Mails** können Sie Zustell- und Statusinformationen über Nachrichten abrufen, die an Ihr Unternehmen gesendet wurden.
Zusammenfassung der ausgehenden E-Mails	Mit dem Portlet **Zusammenfassung der ausgehenden E-Mails** können Sie Zustell- und Statusinformationen über Nachrichten abrufen, die von Ihrem Unternehmen aus gesendet wurden.
SMTP-Entdeckungen	Mit dem Portlet **SMTP-Entdeckungen** können Sie die Gesamtanzahl der Nachrichten feststellen, die eine Entdeckung basierend auf Absender, Verbindung, Empfänger oder Inhalt ausgelöst haben, bzw. Daten zum eingehenden oder ausgehenden SMTP-Datenverkehr anzeigen.
POP3-Entdeckungen	Mit dem Portlet **POP3-Entdeckungen** können Sie anzeigen, wie viele Nachrichten eine Entdeckung basierend auf Bedrohungen wie Viren, Komprimierungsprogrammen oder potenziell anstößigen Bildern ausgelöst haben.
Systemzusammenfassung	Mit dem Portlet **Systemzusammenfassung** können Sie Informationen über den Lastausgleich, den für jede Partition verwendeten Speicherplatz, die gesamte CPU-Auslastung, den verwendeten und verfügbaren Arbeitsspeicher sowie Swap-Details anzeigen.
Hardware-Zusammenfassung	Das Portlet **Hardware-Zusammenfassung** verwendet Statusindikatoren, um den Status von Netzwerkschnittstellen, USV-Servern, des Bridge-Modus (sofern aktiviert) sowie den RAID-Status anzuzeigen.
Netzwerkzusammenfassung	Mit dem Portlet **Netzwerkzusammenfassung** können Sie Informationen über den Status Ihrer Verbindungen, den Netzwerkdurchsatz und Zähler in Bezug auf die Kernel-Modus-Blockierung anzeigen.
Dienste	Mit dem Portlet **Dienste** können Sie Statistiken zum Aktualisierungs- und Dienststatus anzeigen, die auf den von der Appliance verwendeten Protokoll- und externen Servern basieren.

Option	Beschreibung
Clustering	Mit dem Portlet **Clustering** können Sie nach der Konfiguration Ihrer Appliance als Bestandteil eines Clusters oder bei Verwendung der Blade-Server-Hardware Informationen über den gesamten Cluster bereitstellen.
Tasks	Mit dem Portlet **Tasks** gelangen Sie direkt zu den Bereichen der Benutzeroberfläche, in denen Sie die Nachrichtenwarteschlange durchsuchen, Berichte anzeigen, Richtlinien verwalten, E-Mail-Protokoll-, Netzwerk- und System-Einstellungen konfigurieren und auf Funktionen zur Fehlerbehebung zugreifen können.

5 Testen der Konfiguration

Diese Informationen beschreiben, wie Sie testen können, ob die Appliance nach der Installation ordnungsgemäß funktioniert.

Inhalt

Vorgehensweise – Testen der Verbindung

Gehen Sie wie nachfolgend beschrieben vor, um die grundlegende Verbindungsfähigkeit zu bestätigen.

Das McAfee Email Gateway prüft, ob es mit dem Gateway kommunizieren und Server sowie DNS-Server aktualisieren kann. Außerdem wird überprüft, ob der Name der Appliance und der Name der Domäne gültig sind.

Vorgehensweise

1. Wählen Sie in der Navigationsleiste die Option **Fehlerbehebung**, oder wählen Sie im Dashboard im Bereich **Tasks** die Option **Systemtests ausführen**.
2. Klicken Sie auf die Registerkarte **Tests**.
3. Klicken Sie auf **Tests starten**.

Jeder Test sollte positiv beendet werden.

Vorgehensweise – Die DAT-Dateien aktualisieren

Gehen Sie wie nachfolgend beschrieben vor, um sicherzustellen, dass das McAfee Email Gateway über die aktuellsten Erkennungsdefinitionsdateien (DAT) verfügt. Es wird empfohlen, dass Sie diese aktualisieren, bevor Sie die Scan-Optionen konfigurieren.

Im Rahmen der Verwendung des McAfee Email Gateway können Sie einzelne Arten von Definitionsdateien aktualisieren sowie die standardmäßig geplanten Aktualisierungen an Ihre Anforderungen anpassen.

Vorgehensweise

1. Wählen Sie **System** | **Komponentenverwaltung** | **Aktualisierungsstatus**.
2. Klicken Sie zum Aktualisieren des Antiviren-Moduls und der Antiviren-Datenbank auf **Jetzt aktualisieren**.

   Für die Überprüfung, ob das Update korrekt angewendet wurde, öffnen Sie das Portlet **Dienste** im Dashboard, und erweitern Sie den Status für **Aktualisierungen**. Die Antiviren-Komponenten haben einen grünen Status.

Vorgehensweise – Testen von E-Mail-Verkehr und Virenerkennung

Gehen Sie wie nachfolgend beschrieben vor, um zu überprüfen, ob der E-Mail-Verkehr erfolgreich durch das McAfee Email Gateway geleitet wird und ob dabei Gefahren ordnungsgemäß identifiziert werden. Wir verwenden die EICAR-Testdatei, eine harmlose Datei, die eine Virenerkennung auslöst.

Vorgehensweise

1. Senden Sie eine E-Mail von einem externen E-Mail-Konto (wie Hotmail) an einen internen Posteingang, und vergewissern Sie sich, dass die E-Mail angekommen ist.
2. Sehen Sie sich im Dashboard die Bereiche mit den Erkennungen an. Aus der Liste für das Protokoll, das Sie zum Versenden der Nachricht verwendet haben, sollte hervorgehen, dass eine Nachricht empfangen wurde.
3. Kopieren Sie die folgende Zeile in eine Datei, und achten Sie dabei darauf, dass Sie keine Leerzeichen oder Zeilenumbrüche hinzufügen:

   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
4. Speichern Sie die Datei unter dem Namen EICAR.COM.

   Abhängig von Ihrer lokalen Antiviren-Software und -Konfiguration kann dies zu einer Entdeckung und Isolierung auf Ihrem lokalen Rechner führen.
5. Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine Nachricht mit der Datei EICAR.COM als Anhang, und senden Sie die Nachricht an einen internen Posteingang.
6. Kehren Sie zum Dashboard zurück, und sehen Sie sich die Bereiche mit den Erkennungen an. Sie sollten sehen, dass ein Virus erkannt wurde.
7. Löschen Sie die Nachricht, wenn Sie das Testen Ihrer Installation abgeschlossen haben, damit ahnungslose Benutzer keinen Schreck bekommen.

Vorgehensweise – Testen der Spam-Erkennung

Gehen Sie wie nachfolgend beschrieben vor, um einen *General Test mail for Unsolicited Bulk Email* (Allgemeiner Test auf unerwünschte Bulk-E-Mails, GTUBE) auszuführen, mit dem geprüft wird, ob das McAfee Email Gateway eingehende Spam-Mail erkennt.

Vorgehensweise

1. Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine neue E-Mail.
2. Kopieren Sie den folgenden Text in den Nachrichtenteil der E-Mail:

   XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

   Achten Sie darauf, dass der Text keine Zeilenumbrüche enthält.
3. Senden Sie die neue E-Mail an eine interne Posteingangsadresse.

   Das Gerät scannt die Nachricht, erkennt sie als Junk-E-Mail und verarbeitet sie entsprechend. Der GTUBE-Test hat Vorrang vor Blacklists und Whitelists.

   Nähere Informationen zum GTUBE-Test finden Sie unter http://spamassassin.apache.org/tests.html.

6 Erkunden der Funktionen der Appliance

Diese Informationen enthalten Vorgehensweisen zur Demonstration der ausgeführten Scan-Funktionen von McAfee Email Gateway. Sie werden detailliert durch das Erstellen und Testen einiger Beispielrichtlinien geführt und erfahren, wie Sie die relevanten Berichte generieren.

Einführung in die Richtlinien

Die Appliance verwendet Richtlinien zur Beschreibung der Aktionen, die die Appliance bei Bedrohung durch Viren, Spam, unerwünschte Dateien und Verlust kritischer Informationen ausführen muss.



Email | Email Policies

Richtlinien sind Sammlungen von Regeln oder Einstellungen, die auf bestimmte Arten von Datenverkehr oder auf Benutzergruppen angewendet werden können.

Verschlüsselung

Auf den Seiten **Verschlüsselung** können Sie McAfee Email Gateway für die Verwendung unterstützter Verschlüsselungsverfahren konfigurieren, damit E-Mail-Nachrichten sicher zugestellt werden.



E-Mail | Verschlüsselung

Das McAfee Email Gateway umfasst mehrere Verschlüsselungs-Methoden und kann dafür eingerichtet werden, anderen Scan-Funktionen Verschlüsselungsdienste zur Verfügung zu stellen. Es kann jedoch auch als reiner Verschlüsselung-Server nur für die Verschlüsselung von E-Mails verwendet werden.

Vorgehensweise – Verschlüsseln des gesamten E-Mail-Verkehrs mit einem bestimmten Kunden

Eine häufige Art der Nutzung von Verschlüsselungsfunktionen besteht in der Konfiguration einer Richtlinie, die festlegt, dass die Verschlüsselung nur für E-Mail-Nachrichten an einen bestimmten Kunden verwendet werden soll.

Die folgenden Vorgehensweisen zeigen auf, wie das McAfee Email Gateway so konfiguriert wird, dass alle E-Mail-Nachrichten, die an einen bestimmten Kunden gerichtet sind, verschlüsselt gesendet werden.

Vorgehensweise – Erstellen einer neuen Richtlinie

Erfahren Sie, wie Sie eine neue Scan-Richtlinie erstellen können.

Ihre Appliance scannt die über sie versendeten E-Mail-Nachrichten anhand der von Ihnen erstellten Richtlinien. Sie können mehrere Richtlinien erstellen, um zu steuern, wie unterschiedliche Benutzer E-Mail verwenden, oder um verschiedene Aktionen anzugeben, die abhängig von verschiedenen Bedingungen ausgeführt werden sollen.

Vorgehensweise

1. Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien.**
2. Wählen Sie das erforderliche Protokoll aus, indem Sie die Schritte unter *Vorgehensweise – Anzeigen der Richtlinien für SMTP, POP3 bzw. McAfee Secure Web Mail* ausführen.
3. Klicken Sie auf **Richtlinie hinzufügen**.
4. Geben Sie auf der Seite **Scan-Richtlinien – Neue Richtlinie** folgende Informationen an:
   a. Einen Namen für die Richtlinie.
   b. Geben Sie eine optionale Beschreibung für die neue Richtlinie ein.
   c. Geben Sie an, woher sich die Einstellungen der neuen Richtlinie ableiten.

      
      Wenn Sie bereits eine ähnliche Richtlinie eingerichtet haben, wählen Sie diese aus, um deren Einstellungen in die neue Richtlinie zu übernehmen.

   d. Wählen Sie aus, ob die Richtlinie auf ein- oder ausgehenden E-Mail-Verkehr angewendet werden soll. (Nur SMTP)
   e. Wählen Sie die erforderliche **Übereinstimmungs-Logik** für die Richtlinie aus.
   f. Wählen Sie den Regeltyp aus, wählen Sie, wie die Regel übereinstimmen sollte, und wählen Sie den Wert aus, gegen den die Regel testet.
   g. Falls erforderlich, fügen Sie zusätzliche Regeln hinzu, und verwenden Sie die Schaltflächen ⇧ und ⇩, um die Regeln in die richtige Reihenfolge zu bringen.
5. Klicken Sie auf **OK**.

Die neue Richtlinie wird an den Anfang der Richtlinienliste gesetzt.

Vorgehensweise – Konfigurieren der Verschlüsselungseinstellungen

Konfigurieren Sie das McAfee Email Gateway für die Verwendung von Verschlüsselung.

Vorgehensweise

1. Wählen Sie **E-Mail | Verschlüsselung | Secure Web Mail | Grundlegende Einstellungen.**
2. Wählen Sie **Secure Web Mail-Client aktivieren.**
3. Wählen Sie **E-Mail | Verschlüsselung | Secure Web Mail | Benutzerkontoeinstellungen.**

   
   Empfänger werden automatisch angemeldet und erhalten eine digital signierte Benachrichtigung im HTML-Format. Der Administrator wählt, ob eine Push- und/oder eine Pull-Verschlüsselung vorgenommen wird.

4. Wählen Sie **E-Mail | Verschlüsselung | Secure Web Mail | Kennwortverwaltung.**

   
   Die minimale Kennwortlänge beträgt acht Zeichen. Das Kennwort läuft nach 365 Tagen ab.

Task – Aktivieren der Verschlüsselung für Nachrichten, die mit einer Compliance-Regel übereinstimmen

Aktivieren Sie die erforderliche Verschlüsselungsfunktion auf Ihrem McAfee Email Gateway für Nachrichten, die mit einer Compliance-Regel übereinstimmen.

In diesem Beispiel werden Nachrichten verschlüsselt, die mit der HIPAA-Compliance-Regel übereinstimmen.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance**.
2. Klicken Sie auf **Compliance aktivieren**, und wählen Sie **Neue Regel aus Vorlage erstellen**.
3. Suchen Sie die Regel **HIPAA-Compliance**, und wählen Sie sie aus.
4. Klicken Sie auf **Weiter**, um jeweils zur nächsten Assistentenseite zu gelangen.
5. Wählen Sie als primäre Aktion **Durchlassen (Überwachen)**.
6. Wählen Sie unter **Und auch** die Option **Nachricht verschlüsselt zustellen**.
7. Klicken Sie auf **Fertigstellen**, und klicken Sie dann auf **OK**, um das Dialogfeld zu schließen.
8. Wählen Sie **Email | Email Policies | Policy Options | Encryption**.
9. Wählen Sie unter **Verschlüsselungszeitpunkt** die Option **Nur wenn von einer Scan-Aktion ausgelöst**.
10. Wählen Sie unter **Optionen zur integrierten Verschlüsselung** die Option **Secure Web Mail**, und klicken Sie auf **OK**.
11. Übernehmen Sie die Änderungen.

Vorgehensweise – Erkennen von isolierten E-Mail-Nachrichten

Gehen Sie wie nachfolgend beschrieben vor, um nach E-Mails zu suchen, die von Ihrer McAfee Email Gateway Appliance isoliert wurden.

So zeigen Sie eine Liste aller isolierten Nachrichten an:

Vorgehensweise

1. Klicken Sie auf **Berichte | Nachrichtensuche**.
2. Wählen Sie **Isoliert** in der Dropdown-Liste **Nachrichtenstatus** aus.
3. Klicken Sie auf **Suchen/Aktualisieren**.

Alle isolierten Nachrichten werden im unteren Bereich der Seite angezeigt.

Vorgehensweise – Eingrenzen der Suche

Sie können die Suche nach isolierten E-Mails weiter eingrenzen, sodass nur Nachrichten angezeigt werden, die aufgrund von bestimmten Auslösern isoliert wurden. Gehen Sie in diesem Beispiel wie folgt vor, um die E-Mails zu finden, die aufgrund von Compliance-Problemen in die Quarantäne verschoben wurden:

Vorgehensweise

1. Führen Sie die unter *Vorgehensweise – Ermitteln, welche E-Mails isoliert sind* beschriebenen Schritte aus.
2. Wählen Sie **Compliance** in der Dropdown-Liste **Kategorie** aus.
3. Klicken Sie auf **Suchen/Aktualisieren**.

Der untere Bereich des Bildschirms wird aktualisiert und zeigt nur die Nachrichten an, die aufgrund von Compliance-Problemen isoliert wurden.

Vorgehensweise – Anzeigen einer bestimmten E-Mail-Nachricht

Sie können den Inhalt einer isolierten E-Mail sehen.

Vorgehensweise

1. Führen Sie die Schritte unter *Vorgehensweise – Eingrenzen der Suche* aus.
2. Aktivieren Sie links auf der Seite das Kontrollkästchen, um die entsprechende isolierte Nachricht auszuwählen.
3. Klicken Sie auf **Nachricht anzeigen**.

Die ausgewählte Nachricht wird in einem neuen Fenster angezeigt. In diesem Fenster können Sie den Inhalt der E-Mail lesen. Außerdem können Sie alternativ die detaillierten Informationen des E-Mail-Headers anzeigen. Nachdem Sie die Nachricht gelesen haben, können Sie weitere Aktionen für die E-Mail auswählen, indem Sie auf die entsprechenden Schaltflächen klicken.

Vorgehensweise – Freigeben einer isolierten E-Mail-Nachricht

Nachdem Sie die isolierte E-Mail-Nachricht gesehen haben, möchten Sie möglicherweise die Nachricht aus der Quarantäne freigeben. Gehen Sie dazu folgendermaßen vor.

So entlassen Sie eine ausgewählte Nachricht aus der Quarantäne

Vorgehensweise

1. Führen Sie die Schritte unter *Vorgehensweise – Anzeigen einer bestimmten E-Mail-Nachricht* aus.
2. Klicken Sie auf **Ausgewählte Elemente aus Quarantäne entlassen**.

Die ausgewählte E-Mail wird aus der Quarantäne entlassen.



E-Mails mit infiziertem Inhalt können nicht aus der Quarantäne entlassen werden, da dies Schäden auf Ihren Systemen verursachen könnte.

Compliance-Einstellungen

Über diese Seite können Sie Compliance-Regeln erstellen und verwalten.



Email | **Email Policies** | **Compliance** | **Compliance**

Vorteile der Compliance-Einstellungen

Verwenden Sie Compliance-Scans zur Unterstützung der Compliance mit gesetzlichen und betrieblichen Auflagen. Sie können aus einer Bibliothek aus vordefinierten Compliance-Regeln wählen oder eigene Regeln und Wörterbücher für Ihr Unternehmen erstellen.

Compliance-Regeln können hinsichtlich ihrer Komplexität von einem einfachen Auslöser bei der Erkennung eines einzelnen Begriffs in einem Wörterbuch bis hin zum Aufbauen auf und Kombinieren von faktorbasierten Wörterbüchern variieren, die nur auslösen, wenn ein bestimmter Schwellenwert erreicht wird. Mithilfe der erweiterten Funktionen von Compliance-Regeln können Wörterbücher mit den logischen Operationen *eines von*, *alle von* oder *außer* kombiniert werden.

Vorgehensweise – Beschränken des Faktorbeitrags eines Wörterbuchbegriffs

Gehen Sie wie nachfolgend beschrieben vor, um den Faktorbeitrag eines Wörterbuchbegriffs zu beschränken.

> **Bevor Sie beginnen**
>
> Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch **Vergütung und Leistungen**.

Sie können beschränken, wie oft ein Begriff zum Gesamtfaktor beitragen kann.

Wenn beispielsweise "Testbegriff" in einem Wörterbuch den Faktor 10 hat und fünfmal in einer E-Mail erkannt wird, wird 50 zum Gesamtfaktor addiert. Alternativ können Sie eine Beschränkung festlegen, sodass beispielsweise nur zwei Vorkommnisse zum Gesamtwert beitragen, indem Sie für "Max. Begriffsanzahl" den Wert "2" angeben.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance**.
2. Erweitern Sie die Regel, die Sie bearbeiten möchten, und klicken Sie anschließend auf das Symbol **Bearbeiten** neben dem Wörterbuch, dessen Faktor Sie ändern möchten.
3. Geben Sie unter **Max. Begriffsanzahl** die maximale Anzahl an Vorkommnissen eines Begriffs an, die zum Gesamtfaktor beitragen sollen.

Vorgehensweise – Bearbeiten des einer vorhandenen Regel zugewiesenen Schwellenwerts

Gehen Sie wie nachfolgend beschrieben vor, um den Schwellenwert zu bearbeiten, der einer vorhandenen Regel zugeordnet ist.

> **Bevor Sie beginnen**
>
> Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch **Vergütung und Leistungen**.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance**.
2. Erweitern Sie die Regel, die Sie bearbeiten möchten, und wählen Sie anschließend das Symbol **Bearbeiten** neben dem Wörterbuch aus, dessen Faktor Sie ändern möchten.
3. Geben Sie unter **Schwellenwert für Wörterbuch** den Faktor ein, bei dem die Regel ausgelöst werden soll, und klicken Sie auf **OK**.

Vorgehensweise – Definieren einer Regel zum Überwachen oder Blockieren bei Erreichen eines Schwellenwerts

Bei faktorbasierten Wörterbüchern kann es sinnvoll sein, Auslöser zu überwachen, die einen niedrigen Schwellenwert erreichen, und die E-Mails nur zu blockieren, wenn ein hoher Schwellenwert erreicht wird.

Vorgehensweise

1 Wählen Sie **Email | Email Policies | Compliance**.

2 Klicken Sie auf **Neue Regel erstellen**, geben Sie einen Namen für die Regel ein, beispielsweise `Unzufriedenheit - Niedrig`, und klicken Sie auf **Weiter**.

3 Wählen Sie das Wörterbuch **Unzufriedenheit** aus, und geben Sie unter **Schwellenwert** den Wert `20` ein.

4 Klicken Sie auf **Weiter** und anschließend erneut auf **Weiter**.

5 Akzeptieren Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Standardaktion.

6 Klicken Sie auf **Fertig stellen**.

7 Wiederholen Sie die Schritte 2 bis 4, um eine weitere neue Regel zu erstellen. Nennen Sie diese jedoch `Unzufriedenheit - Hoch`, und weisen Sie ihr den Schwellenwert 40 zu.

8 Wählen Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Option **Verbindung verweigern (Blockieren)** aus.

9 Klicken Sie auf **Fertig stellen**.

10 Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

Vorgehensweise – Hinzufügen eines Wörterbuchs zu einer Regel

Gehen Sie wie folgt vor, um ein neues Wörterbuch zu einer vorhandenen Regel hinzuzufügen.

Vorgehensweise

1 Wählen Sie **Email | Email Policies | Compliance**.

2 Erweitern Sie die Regel, die Sie bearbeiten möchten.

3 Wählen Sie **Wörterbuch hinzufügen**.

4 Wählen Sie das neue Wörterbuch aus, das Sie hinzufügen möchten, und klicken Sie auf **OK**.

Vorgehensweise – Erstellen einer komplexen benutzerdefinierten Regel

Gehen Sie wie nachfolgend beschrieben vor, um eine komplexe Regel zu erstellen, die auslöst, wenn sowohl Wörterbuch A als auch Wörterbuch B erkannt werden, jedoch nicht, wenn darüber hinaus auch Wörterbuch C erkannt wird.

Vorgehensweise

1 Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien** , und wählen Sie **Compliance**.

2 Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

3 Klicken Sie auf **Neue Regel erstellen**, um den **Assistenten für die Regelerstellung** zu öffnen.

4 Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.

5 Wählen Sie zwei Wörterbücher aus, die in die Regel aufgenommen werden sollen, und klicken Sie auf **Weiter**.

6 Wählen Sie in der Ausschlussliste ein Wörterbuch aus, das Sie von der Regel ausschließen möchten.

7 Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn die Regel ausgelöst wird.

8 Wählen Sie in der Dropdown-Liste **Und bedingt** die Option **Alle** aus, und klicken Sie auf **Fertig stellen**.

Vorgehensweise – Erstellen einer einfachen benutzerdefinierten Regel

Gehen Sie wie nachfolgend beschrieben vor, um eine einfache benutzerdefinierte Regel zu erstellen, die Nachrichten blockiert, die Sozialversicherungsnummern enthalten.

Vorgehensweise

1. Wählen Sie **Email** | **Email Policies** | **Compliance**.
2. Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Neue Regel erstellen**, um den **Assistenten für die Regelerstellung** zu öffnen.
4. Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.
5. Geben Sie im Suchfeld `sozial` ein.
6. Wählen Sie das Wörterbuch **Sozialversicherungsnummer** aus, und klicken Sie zweimal auf **Weiter**.
7. Wählen Sie die Aktion **Verbindung verweigern (Blockieren)** aus, und klicken Sie auf **Fertig stellen**.

Vorgehensweise – Blockieren von Nachrichten, die gegen eine Richtlinie verstoßen

Gehen Sie wie nachfolgend beschrieben vor, um E-Mail-Nachrichten zu blockieren, die die Richtlinie "Bedrohliche Sprache" verletzen.

Vorgehensweise

1. Wählen Sie **Email** | **Email Policies** | **Compliance**.
2. Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Neue Regel aus Vorlage erstellen**, um den **Assistent für die Regelerstellung** zu öffnen.
4. Wählen Sie die Richtlinie **Zulässige Nutzung - Bedrohliche Sprache** aus, und klicken Sie auf **Weiter**.
5. Sie können den Namen der Regel optional ändern. Klicken Sie anschließend auf **Weiter**.
6. Ändern Sie die primäre Aktion in **Verbindung verweigern (Blockieren)**, und klicken Sie auf **Fertig stellen**.
7. Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

Data Loss Prevention-Einstellungen

Auf dieser Seite können Sie eine Richtlinie erstellen, die Data Loss Prevention-Aktionen für die Kategorien der registrierten Dokumente zuweist.


Email | **Email Policies** | **Compliance** | **Data Loss Prevention**

Vorteile des Einsatzes von Data Loss Prevention (DLP)

Mit der Data Loss Prevention-Funktion können Sie den Fluss kritischer Informationen beschränken, die in E-Mail-Nachrichten per SMTP über die Appliance gesendet werden. Sie können beispielsweise die Übertragung eines kritischen Dokuments, wie z. B. eines Finanzberichts, blockieren, das an eine Adresse außerhalb Ihres Unternehmens gesendet werden soll. Die Erkennung erfolgt, sobald das Originaldokument als E-Mail-Anhang oder als Textausschnitt aus dem Originaldokument versendet wird.

Die DLP-Konfiguration erfolgt in zwei Phasen:

- Registrierung der Dokumente, die geschützt werden sollen
- Aktivieren der DLP-Richtlinie und Kontrollieren der Erkennung (dieses Thema)



Wenn ein hochgeladenes registriertes Dokument eingebettete Dokumente enthält, wird von deren Inhalt ebenfalls ein Fingerabdruck angelegt. Wenn später während eines Scans der Übereinstimmungsprozentsatz berechnet wird, wird der kombinierte Inhalt verwendet. Wenn eingebettete Dokumente separat behandelt werden sollen, müssen sie separat registriert werden.

Vorgehensweise – Verhindern, dass ein vertrauliches Dokument gesendet wird

Im Folgenden erfahren Sie, wie Sie verhindern, dass vertrauliche Finanzdokumente aus Ihrem Unternehmen heraus gesendet werden.

Bevor Sie beginnen

In diesem Beispiel wird davon ausgegangen, dass Sie bereits die Kategorie "Finanzen" erstellt haben.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance | Data Loss Prevention**.
2. Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Neue Regel erstellen**, wählen Sie die Kategorie "Finanzen" aus, und klicken Sie auf **OK**, damit die Kategorie in der Liste **Regeln** angezeigt wird.
4. Wählen Sie die der Kategorie zugeordnete Aktion aus, ändern Sie die primäre Aktion in **Verbindung verweigern (Blockieren)**, und klicken Sie auf **OK**.
5. Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

Vorgehensweise – Blockieren des Versendens eines Dokumentabschnitts

Gehen Sie wie nachfolgend beschrieben vor, um zu verhindern, dass auch nur ein kleiner Abschnitt eines Dokuments aus Ihrem Unternehmen heraus gesendet wird.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance | Data Loss Prevention**.
2. Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.
3. Aktivieren Sie die Einstellung für aufeinander folgende Signaturen, und geben Sie die Anzahl an aufeinander folgende Signaturen ein, bei der die DLP-Richtlinie eine Erkennung auslösen soll. Der Standardwert ist **10**.
4. Klicken Sie auf **Neue Regel erstellen**, wählen Sie die Kategorie "Finanzen" aus, und klicken Sie auf **OK**, damit die Kategorie in der Liste "Regeln" angezeigt wird.
5. Wählen Sie die der Kategorie zugeordnete Aktion aus, ändern Sie die primäre Aktion in **Verbindung verweigern (Blockieren)**, und klicken Sie auf **OK**.
6. Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

Vorgehensweise – Ausschließen eines bestimmten Dokuments für eine Richtlinie

Gehen Sie wie nachfolgend beschrieben vor, um zu verhindern, dass ein bestimmtes Finanzdokument die DLP-Richtlinieneinstellungen auslöst.

Vorgehensweise

1. Wählen Sie **Email | Email Policies | Compliance | Data Loss Prevention**.
2. Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Dokumentausschluss erstellen**, wählen Sie das Dokument aus, das von dieser Richtlinie ignoriert werden soll, und klicken Sie auf **OK**.
4. Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

7 Zusätzliche Konfigurationsoptionen

Diese Informationen geben Ihnen einige Tipps zu bewährten Vorgehensweisen und stellen Ihnen einige erweiterte Konfigurationsoptionen vor.

Inhalt

Task – Durchführen eines Upgrades auf die aktuelle Version von McAfee Email Gateway Virtual Appliance

Führen Sie anhand dieser Vorgehensweise ein Upgrade auf die aktuelle Version von McAfee Email Gateway Virtual Appliance auf McAfee Email Gateway Virtual Appliance Version 7.0.2 (oder höher) unter Verwendung des .ISO-Images der Software durch.

Bevor Sie beginnen

McAfee Email Gateway Virtual Appliance Version 7.0.2 (oder höher) muss auf Ihrem System bereits installiert und konfiguriert sein.

Nachdem ein Betriebssystem auf einer virtuellen Appliance installiert wurde, startet die virtuelle Maschine immer zuerst direkt von der Festplatte. Um diese Funktion zu umgehen, müssen Sie die virtuelle Maschine herunterfahren und eine Startverzögerung beim Hochfahren konfigurieren, so dass Sie genügend Zeit haben, auf das **Boot**-Menü zuzugreifen und stattdessen das Starten über die Installations-CD zu veranlassen.

Vorgehensweise

1. Laden Sie die .ISO-Upgrade-Datei der McAfee Email Gateway Virtual Appliance von der McAfee-Download-Webseite herunter, und extrahieren Sie sie.
2. Fahren Sie die virtuelle Appliance herunter.
   a. Melden Sie sich bei der Benutzeroberfläche der virtuellen Appliance an, und wählen Sie **System** | **Systemverwaltung** | **Systembefehle**.
   b. Geben Sie das Kennwort ein.
   c. Wählen Sie **Appliance beenden**.
3. Melden Sie sich beim VMware ESX-Server an, oder verwenden Sie den VMware Infrastructure Client bzw. den VMware vSphere Client, um sich beim VMware Virtual Center Server anzumelden.

4 Aktivieren Sie eine **Power-on-Boot**-Verzögerung, damit Sie ausreichend Zeit haben, die virtuelle Maschine von der CD aus starten zu lassen:

   a Wählen Sie die virtuelle Appliance in Liste **Inventory** (Inventar), und klicken Sie auf **Summary** (Zusammenfassung).

   b Wählen Sie **Edit Settings | Options | Boot Options** (Einstellungen bearbeiten | Optionen | Boot-Optionen).

   c Geben Sie unter **Power-on-Boot** (Power-on-Boot-Verzögerung) `10,000` in das Textfeld ein, und klicken Sie auf **OK**.

5 Schalten Sie die virtuelle Appliance ein.

6 Stellen Sie sicher, dass sich der Mauszeiger in der Konsole der virtuellen Appliance befindet. Drücken Sie anschließend die ESC-Taste, um das **Boot Menu** (Boot-Menü) zu öffnen.



Wählen Sie noch keine Optionen.

7 Ziehen Sie den Mauszeiger aus der Konsole, und wählen Sie **Connect CD/DVD1** (CD/DVD1 verbinden).

8 Navigieren Sie zu dem Ordner, in den Sie die McAfee Email Gateway Virtual Appliance .ISO-Datei heruntergeladen haben, und doppelklicken Sie auf **<McAfee-MEG 7.x-<build-number>.VMbuy.iso>**.

9 Wenn die ISO-Datei verbunden ist, klicken Sie erneut auf das Konsolenfenster. Wählen Sie **CD-ROM Drive** (CD-ROM-Laufwerk) aus, und drücken Sie die `EINGABE`-Taste.

10 Die virtuelle Appliance startet von der ISO-Datei.

11 Geben Sie **j** ein, um den Bedingungen der Endbenutzer-Lizenzvereinbarung zuzustimmen.

12 Wählen Sie die gewünschte Upgrade-Option, und drücken Sie die `Eingabetaste`, um das Upgrade durchzuführen.

13 Geben Sie **j** ein, um zu bestätigen, dass Sie fortfahren möchten.

Vorgehensweise – Ändern der standardmäßigen Aktionen zum Ausschalten und Zurücksetzen

Ändern Sie anhand dieser Vorgehensweise die Aktionen zum **Ausschalten** und **Zurücksetzen** in VMware vSpere, sodass die McAfee Email Gateway Virtual Appliance heruntergefahren werden kann, ohne dass das Dateisystem der virtuellen Maschine beschädigt wird.

Vorgehensweise

1 Klicken Sie im **VMware vSphere Client** mit der rechten Maustaste auf die McAfee Email Gateway Virtual Appliance, und wählen Sie **Einstellungen bearbeiten** aus.

2 Wählen Sie die Registerkarte **Options** (Optionen), und wählen Sie **VMware Tools**.

3 Setzen Sie die Option neben dem roten Kästchen auf **Shut Down Guest** (Gast herunterfahren).

4 Setzen Sie die Option neben dem Symbol **Reset** (Zurücksetzen) (roter und grüner Pfeil) auf **Restart Guest** (Gast neu starten).

Vorgehensweise – Konfigurieren der Optionen zum Herunterfahren und Neustart

Nutzen Sie diese Vorgehensweise, um McAfee Email Gateway Virtual Appliance so zu konfigurieren, dass sie automatisch heruntergefahren und neu gestartet wird, wenn Sie VMware vSphere neu starten.

Vorgehensweise

1. Wählen Sie den vSphere-Host aus, und klicken Sie auf die Registerkarte **Configuration** (Konfiguration).
2. Wählen Sie **Start/Herunterfahren der virtuellen Maschine** im Feld „Software" aus, klicken Sie auf **Eigenschaften** und führen Sie folgende Schritte aus:
   - Aktivieren Sie die Option **Allow virtual machines to start and stop automatically with the system** (Virtuellen Maschinen das automatische Starten und Anhalten mit dem System erlauben).
   - Ändern Sie die **Shutdown Action** (Aktion bei Herunterfahren) in **Guest Shutdown** (Gast herunterfahren).
3. Wählen Sie McAfee Email Gateway Virtual Appliance aus der Liste, und klicken Sie auf **Nach oben**, bis es an oberster Stelle in der Liste erscheint.
4. Klicken Sie auf **Bearbeiten**.
5. Wählen Sie unter **Virtual Machine Autostart Settings** (Autostart-Einstellungen für die virtuelle Maschine) im Feld **Shutdown Settings** (Einstellungen für Herunterfahren) die Option **Use specified settings** (Angegebene Einstellungen verwenden) aus, und wählen Sie dann **Guest Shutdown** (Gast herunterfahren) neben **Perform shutdown action** (Aktion zum Herunterfahren durchführen).
6. Klicken Sie zwei Mal auf **OK**, um das Konfigurationsfenster zu schließen.

Die virtuelle Appliance wird nun in der Liste unter der Überschrift **Automatic Startup** (Automatischer Start) angezeigt, und der Wert in der Spalte **Shutdown** (Herunterfahren) lautet **Shut down guest** (Gast herunterfahren).

Index

